TOP10VPN | Digital Rights Research Grant

August 2021

China's Surveillance State: A Global Project

How American and Chinese companies collaborate in the construction and global distribution of China's information control apparatus.

Authors

Valentin Weber
Vasilis Ververis

Editor

Samuel Woodhams

Table of Contents

Since its inception in 1998, the Golden Shield Project (GSP), China's digital surveillance programme, has changed dramatically in sophistication and scale. To give an example, around the turn of the millennium, the GSP's aim to establish a nationwide CCTV network was still in an early stage. Shenzhen-based Hikvision, the world's largest CCTV manufacturer, was only founded in November 2001. The sophistication of technologies was also still nascent. Cameras with infrared capabilities had only started to become more widely adopted, which allowed for night-time surveillance.

The early characteristics of China's GSP are well captured in Greg Walton's seminal report China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China. The report showed that American companies had helped build the Chinese surveillance apparatus. This assistance continues until the present day. As our report shows, Cisco, Dell, HP, IBM, Microsoft, and Oracle still supply vital equipment to Chinese police departments across the country.

What is different today, as opposed to 2001 when Walton's report was published, is that throughout the years, the GSP has grown considerably in size and sophistication. New technologies such as facial recognition have allowed for more efficient surveillance. By 2013 China had installed ~30 million surveillance cameras. In 2021, this number has risen to 416 million.

In addition to this, a strong domestic surveillance industry has emerged in China. And now, Chinese companies are exporting the many components that they developed for the GSP to the world. As this report demonstrates, entities based in democracies simply ignore that the Chinese companies they collaborate with also provide technology to the Chinese police and military. Alternatively, it may be that they are simply not aware of those entanglements (one must give them the benefit of doubt). On this note, it is worth mentioning that many of the exports and collaborations occur through third parties and subsidiaries, which complicates due diligence evaluations.

Another distinctive factor in comparison to 2001, is the US's drive for technological decoupling from China, both for geopolitical but also human rights reasons. On the latter note, numerous reports, including this one, have indicated that the GSP has been used in a targeted manner to monitor and suppress the Uyghur ethnic minority in Xinjiang. This suppression has reached genocidal dimensions, according to countries such as the Netherlands, Canada, and the US.

In this report we show how various technologies, including those that may appear benign, such as geolocation technologies, play just as much a role in the Golden Shield Project as a storage server or surveillance cameras, and the associated facial recognition software do. Hence a distinction into less and more harmful technology becomes more blurry.

Emerging technologies, such as surveillance gear, AI, and cybersecurity products, are often labelled as dual- or multi-use in nature. A geolocation product, for example, can be used both to increase efficiency in the agricultural sector and to launch intercontinental ballistic missiles (see UniStrong section). As this report shows, the multi-use nature of technologies is skilfully taken advantage of in companies' marketing strategies. During the research for this paper, many of the English-speaking websites of Chinese companies showcased the civilian application of their products, while the Chinese website also emphasised the surveillance and military applications of products.

What is more, as this report showcases, China's surveillance apparatus directs every industry sector to give data access to authorities. This means that encrypted systems must by law be weakened, i.e, backdoors built in by design. Surveillance ought to be all-encompassing, in the financial sector, in the hotel industry, and on the digital platforms that citizens use to pay taxes. The authors of this report fear that the backdoors that are built into software products at home to monitor citizens (see Aisino section) may be also exported abroad, unless the Chinese Communist Party (CCP) has secretly ordered companies to remove all backdoors when software is sold overseas. The opposite manifests in the Chinese legal framework. China's 2017 National Intelligence Law requires companies to assist the Chinese authorities with intelligence work.

Finally, this report presents a global map of Huawei surveillance middleboxes (devices that monitor and filter internet traffic). We found 1799 such devices to be present worldwide, including in Xinjiang. In total we found Huawei middleboxes to be deployed in 69 countries. These surveillance middleboxes have been used for censorship in 17 countries, including to filter out political content in Burundi, and LGBTQI+ content in Oman. The middleboxes have also been used to power 13 Huawei safe cities in cities as varied as Cochabamba (Bolivia), Lahore (Pakistan), and Nairobi (Kenya).[1] To our knowledge, this research is one of the first to show that these safe cities are up and running and thereby complements media reports that provide scarce information on whether safe cities are already operational or only a project that exists on paper.

Golden Shield Project: A background

This section gives a short overview of the evolution of China's Golden Shield Project from the late 1990s to today.

[1] While recognising the many definitions of safe cities exist and their distinction to smart cities, this report uses the term safe city since Huawei's surveillance middleboxes that run eSight have been specifically linked to safe cities by Huawei.

First phase of the Golden Shield Project

The Ministry of Public Security proposed the GSP in 1998. The GSP's aim has since been to push the public security sector into the information age and thereby increase public security efficiency and meet the growing demands for controlling vast amounts of information. The first phase of the GSP was completed in 2006. One of the major goals of the first phase of the GSP was to create a three-level public security information network (ministry, provinces, cities). During Phase I, eight databases were established

1. National Basic Population Information Resource Database
2. National Entry-Exit Personnel Resource Database
3. National Motor Vehicle/Driver Information Resource Database
4. National Police Officer Information Resource Database
5. National Information Resource Database of Fugitives
6. National Information Resource Database of Offenders and Criminals
7. National Information Resource Database of Stolen Cars
8. National Security Information Resource Database

Second Phase of the Golden Shield Project

The second phase was launched in 2008/2009. While the first phase established the digitisation of the ministry, province and city public security entities, the second phase aims at integrating the three levels of public security network and fostering information sharing between them. China News Service, a state-owned news agency reported how Uyghur protests in July 2009 (at first peaceful but turned violent after Chinese paramilitary used live ammunition against protesters), played an important part in shaping the second phase of the GSP and can be seen as an example of how Chinese authorities used the increasing informatisation of public security forces to quell dissent.

The main goals of the second phase are to introduce a Police Geographic Information System (PGIS), integrate businesses into the public security platform, and increase standardisation of the public security system. The PGIS is a key construction project of the second phase of the GSP. This is also reflected in a 2016 Zhongshan Public Security Bureau procurement document. Tianjin Troila Technology, an information technology company, for instance, created a platform for the PGIS which accomplishes real-time spatial visualisation of data with regards to police work. This use of geo-spatial data, which in its most rudimentary form was introduced into China's public security field in the 1990s, allows police resources to be more efficiently allocated and dispatched. It also facilitates the tracking of vehicles and people of interest and find out interconnections between them.

The Golden Shield Project today

The first and second phase of the GSP have laid the foundation for today's safe cities and its rural equivalent the Sharp Eyes Project. The safe city forms the successor to the first and second phase of the Golden Shield Project. The first pilot projects of safe cities were conducted between 2005-2008, when urban alarm and monitoring systems were installed in several cities. In 2009, IBM was officially lauded for bringing the concept of safe cities to China. A file, which seems to be hosted in IBM's Boulder Data Center mentions that IBM supplied safe city products to the Shandong Provincial Public Security Department, the Harbin Public Security Bureau, the Dalian Public Security Bureau, and the Public Security Department of Liaoning province.

Safe cities rely on integrating business information from hotels, vehicle repair stores, and shopping malls amongst others, and take advantage of data from facial recognition cameras, license plate readers on highways that feed into the public security bureau systems. Safe cities are similar to a body whose sensory neurons (e.g., facial recognition cameras), transmit sensed information through nerve fibres (optical, wireless, and government private networks) to the brain (the Ministry of Public Security's command, dispatch, and decision-making centres). The data that enters the brain is constantly checked against the brain's memory (police cloud; large databases) to identify potentially harmful entities. In the subconscious parts of the brain, linkages between sensory inputs of people, and things are created (hidden information) and future scenarios presented (predictive policing) that go beyond the conscious perception of the brain.

Since its inception in 1998, a complex industrial chain system has formed to make the Golden Shield Project work. It can be divided into a supply and demand side. The supply side consists of the equipment, software, and component manufacturers, as for example, Microsoft, Oracle, Haiyi Software, Huawei, IBM, and UniStrong. The demand side is made up of hotels, machine repair shops, internet service providers (ISPs), and shopping malls, who need to comply with data gathering requirements, as well as over 1,000 police emergency command centres across China that need to make sense of the data.

American metals for China's Golden Shield

From the outset, American companies have played an important role in the construction of the GSP. Cisco's role in providing the necessary routers for blocking websites in particular led Jack Goldsmith and Tim Wu to proclaim that "the Great Wall of China [a subsidiary part of the Golden Shield responsible for censoring information] is, in effect, built with American bricks." As several recent government bidding documents show, American companies' role in supplying technology for the Golden Shield Project continues.

While it is difficult to assess the percentage of American hardware and software used by the Chinese police, one may conclude that it proves crucial for their operation. This is best seen in Windows and Google operating systems (OS).

Windows has a 84% desktop OS market share in China. Although the share in government, party, and military equipment is lower (domestic suppliers seem to dominate with 90% of the market share) the many police procurement documents below mention Windows OS, which shows that the Redmond-designed OS is still wide-spread.

Google's Android OS has a market share of 78.56% in China. It is no surprise then that the app used by Xinjiang police to feed data into the Integrated Joint Platform (IJOP) - which lies at the heart of digital surveillance in Xinjiang - was written for Android OS.

As will be shown below, American products supplied to Chinese police are much more diverse than basic operating systems, and include everything from servers, graphic cards, processors and database management software.

Beijing

A bidding document from 2020 indicates that the Beijing Municipal Public Security Bureau uses Cisco Netflow cards - which can be used for traffic monitoring - IBM servers, Windows 2003 servers and Oracle Database 10g in its systems. The bidding document fits within Project 1203 of the GSP. The main purpose of Project 1203 is improving the network security of China's surveillance architecture, monitoring information flows within the police network system and maintaining identity authentication and access control. It is likely that the above-mentioned Cisco, IBM, Oracle, and Microsoft products will be used towards this purpose.

While providing network security equipment for the Beijing police may seem benign, it is worth remembering that in 2015 this same police agency detained human rights lawyer Wang Quanzhang, allegedly forced him to take medication and tortured him with electrical shocks. In April 2020, Beijing police arrested two amateur computer coders Cai Wei and Chen Mei for having archived censored reports and interviews related to the origins of the virus in Wuhan. One may ask if these events have been considered in the due diligence evaluations of IBM, Microsoft, and Oracle.

Fuzhou, Fujian province

The Fuzhou Public Security Bureau and Zhongshan Public Security documents highlight the use of Oracle, Microsoft and IBM products to power their Public Security Cloud Platform Project (2020). The bidding document shows that those companies' products will be used in a cloud platform that handles, amongst other things, facial recognition, license plate recognition, geo-positioning, and big data policing.

Zhongshan, Guangdong province

Procurement and bidding documents concerning Zhongshan Public Security highlight the use of Oracle, Microsoft and IBM products to be used in conjunction with the Police Geographic Information System (2016) and the Golden Shield Project (2016) more broadly. With regards to the geographic information system, Zhongshan police uses American products to run and maintain a comprehensive police database of streets, sports facilities, residential areas, caves, lakes, tunnels, lamp posts, amongst others. The key goal is for the police to have immediate and up to date information on a certain area to inform police operations.

Nvidia GeForce 605 graphics cards, Intel Core i7 processors, Intel HD graphics processors, Intel H61 motherboard and the Windows 7 OS are named in the technical specifications for the construction of the Zhongshan Patrol Police Command Center (2015), which is part of the second phase of the GSP. The use of American equipment in the command centre is so extensive, that a halt in selling to the Zhongshan police would potentially come at a significant cost for the Zhongshan police. There would be an operational cost, because they could not rely anymore on the most advanced hardware and software, and a financial cost because of having to change major parts of their hardware and software.

Luoyang, Henan province

A Luoyang Public Security Bureau procurement document (2017) mentions that the Bureau's system must be compatible with Oracle, Microsoft, and IBM products - which likely indicates that the police uses these systems to facilitate information exchange between the public security information network and other business networks.

Meanwhile, prominent human rights lawyer Jian Tianyong is under house arrest in Luoyang city and under constant 24/7 surveillance by the Luoyang Public Security Bureau. By providing equipment to Luoyang police, Oracle, Microsoft, and IBM are arguably implicitly endorsing and explicitly empowering their actions.

Urumqi, Xinjiang Uyghur Autonomous Region

Intel core processors have been part of a winning contract to equip the Diwopu International Airport Branch of the Public Security Bureau of Urumqi City, Xinjiang (2020) with electronic equipment. The Intel processors are likely being used for surveillance purposes, since they were bought in conjunction with the Huawei ASG5300 surveillance middlebox.

The Diwopu airport police is crucial to control in Xinjiang. It monitors one of the few international routes into and out of Xinjiang. In 2017, Anar Sabit, an ethnic Kazakh, visited her hometown in Xinjiang. On her way back to Kazakhstan she was denied departure by Diwopu airport border police. They transferred her to an internment camp where authorities

submitted her to political re-education. The main goal of which was to estrange her from her Kazakh cultural heritage.

Daqing, Heilongjiang province

Intel Quad Core processors are listed in the technical specifications of a Daqing City Government Procurement Centre document (2017), Heilongjiang province, for mobile police terminal equipment. As is the Windows 7 OS. In another Daqing City procurement document for a Provincial Video Surveillance Platform (2015) several products appear, including the Database Oracle 11g, Intel Xeon processors, and IBM's Websphere software.

Provincial forensic labs & police departments in China

Cognitech Inc., a company based in Pasadena, California, is an American forensic video analysis company. Its products enable law enforcement to identify vehicles, people, measure objects and subjects (shoulder width, height), deblur license plates and human faces, and enhance resolution on CCTV footage All these video analysis technologies are core to the latest development of the GSP - safe cities.

Cognitech's eclectic customer base includes provincial forensic labs & police departments in China, the US Department of Defense, the US Department of Homeland Security, the FBI, Japan's National Police Agency, and the German Air Force. While specific instances of Cognitech's contracts in China are scant, a 2020 Master's thesis from a student at the People's Public Security University - China's most prominent police academy - claims that Cognitech software is commonly used in China to enhance bad quality footage from police body worn cameras.

How China's Golden Shield companies serve both the Chinese Communist Party and overseas customers

This part of the report presents major players in the Chinese information technology market that have developed technologies for the Golden Shield Project. As the following lines demonstrate, many of the companies have at the same time extensive ties to the police and military (supplying of technologies and collaborations) as well as entities in democracies (exports or collaborations).

H3C: enabling surveillance in Xinjiang and Hong Kong

H3C is a technology company headquartered in Beijing. H3C products range from cloud computing, big data, artificial intelligence, and information security. The company has been deeply involved in nine out of twelve government digitisation projects, including the Golden Shield Project. The H3C website displays that the company supplied the Hong Kong-Zhuhai-Macao bridge IT infrastructure that features an emergency command system,

a passenger inspection centre, and border inspection safety services. With this project H3C aims to “contribute to the image of a powerful China”. Perhaps with a similar mindset H3C has created a dedicated IP telephone network for the Xinjiang Public Security authorities in 2007. In another project H3C products are named in conjunction with a Ili Kazakh Prefecture [Xinjiang] Public Security Bureau project (2021) that pertains to a party-government-military data exchange network.

International involvement

In 2021 H3C appeared in a procurement document that concerns the Hami Municipality [Xinjiang] Public Security Bureau Conference System Operation and Maintenance project (2021), which shows the long-lasting entanglement of the company in Xinjiang public security digitisation projects. The H3C servers supplied for the Hami Municipality conference system use the 2nd Generation Intel Xeon Scalable Processors as well as the Intel Optane DC Persistent Memory Module. Hami Municipality Public Security Bureau is on the US Department of Commerce’s Entity List. What is more, the city Hami harbours a political education camp, which has been associated with torture and ill-treatment of ethnic minority groups.

H3C is a global company, with offices in Hong Kong, Indonesia, Japan, Kazakhstan, Malaysia, Pakistan, Russia, and Thailand. From these offices it covers 100 countries. In Nigeria, H3C equipped airports in Abuja (the capital), Lagos, Port Harcourt, and Kano with equipment that would enable them to run large networks of devices. In this case, the state-owned enterprise China Civil Engineering Construction Corporation - which built these airports - selected H3C for this job. H3C lists partners in Canada, Spain, and Portugal that help distribute H3C products to local markets.

In its corporate social responsibility policy, H3C speaks of cooperating with government and the private sector to ensure “a happy life for everyone”. This corporate policy may appear attractive to international partners and customers, but it turns out to be rather cynical if one considers H3C’s alleged facilitation of oppression of ethnic minority groups in Xinjiang.

DS Communication Equipment Co., Ltd.: Huawei’s partner in the export of safe cities

DS was established in 1993 and is ultimately controlled by the State-owned Assets Supervision and Administration Commission of the State Council (SASAC). For decades, DS has been involved in the GSP. It has developed dispatch systems for the police as well as the first large-scale public security command system in China. Its products have been used by the Shanghai, Nanjing, and Tianjin Public Security Bureau.

International involvement

Its overseas business includes offering a Mobile Police Command System, which allows for an assessment of the position of police forces and street police forces to communicate with the command centre via image, text, voice, and video. DS also sells a predictive policing system designed to forecast the public security situation, criminal behaviour, and the trajectory of people. It is likely that these two technologies are deployed in DS's involvement in the Vientiane City Police Station Command Project (Laos), the Nairobi Emergency Command Center (Kenya), and the Islamabad Emergency Command Center (Pakistan).

DS collaborates closely with Huawei to supply the overseas public security market. In this cooperation, Huawei assures the narrowband and broadband integration, as well as audio- and video integration of products, while DS focuses on the business layer software, i.e. the command management system. DS is present in nearly 20 countries including Guyana, Kenya, Laos, Mauritius, Nigeria, Pakistan, and Suriname. As the company states, it has been committed to expanding the footprint of China's police command system to the world.

Bluedon Information Security Technology: more military than civilian

Bluedon was founded in 1999. It prides itself in having successfully defended over 800 domestic government agencies in 2001 during Sino-American geopolitical tensions. Bluedon refers to what the New York Times labelled the First World Hacker War. In April 2001, an American spy plane and a Chinese jet collided. In the aftermath, Chinese hacktivists faced off American hackers. The result was mutual defacement of websites, and the White House website went down for several hours.

Bluedon has also helped build the GSP. Its AI Firewall product, for instance, is capable of blocking circumvention software, such as Virtual Private Networks. Other products include a web crawler designed for government and military customers that identifies sensitive information on the publicly available internet, and a printing monitoring system for authorities. Information about the company's involvement in the Sharp Eyes Project has largely been deleted from Bluedon's website. Hopewell, a Bluedon-subsidiary, has provided a product that prevents electromagnetic leakage during naval inspections of military weapons systems.

Bluedon subsidiary's products are used during naval inspections of military weapons systems. (Screenshot source)

International involvement

In 2017 Bluedon signed a strategic cooperation agreement with Dell in the context of the "Dell China 4.0 Strategy". During this meeting Dell stated that it hopes to draw on Bluedon's information security expertise. Dell's China 4.0 strategy was announced in 2015. Within the strategy Dell promised to invest $125 billion in China in a 5-year span and co-found the artificial intelligence and advanced computing laboratory with the Chinese Academy of Sciences.

Aisino Aerospace Information Corporation: Xinjiang, the BRI, and backdoors

Aisino Aerospace Information Corporation was established in 2000 and is a subsidiary of the China Aerospace Science and Technology Corporation (CASC). Aisino has been one of the major contributors to the overall design of the GSP, including the construction of the National Population Basic Information Resource Database. This database contains a person's health record and is tied to a unique citizen ID number. It was jointly established by the Ministry of Public Security, the Ministry of Education, the Ministry of Civil Affairs, the Ministry of Human Resources and Social Security, and the National Health and Family Planning Commission.

In 2008, Aisino's Xinjiang subsidiary signed the Xinjiang Police Social Information Collection Platform System Construction Cooperation, which focuses on gathering information through the hotel industry.

In 2013 Aisino subsidiary, Huadi, won a bid to build the Xinjiang Production and Construction Corps Emergency Platform Application System Construction Project. In Huadi's words, the project:

"Will achieve the interoperability among Corps Emergency Platform, the State Council Emergency Platform and Xinjiang Autonomous Region emergency platform and

comprehensively improve Corps' emergency management work capacity… and play a safeguarding role for the reduction of unexpected events and mitigation of their harm, protection of people's lives and property and safeguarding national security, public safety, environmental safety and social order."

In 2018, Aisino built several of the self-service clearance passages for passengers that cross the Hong Kong – Zhuhai – Macao Bridge.

In December 2020, Aisino won a bid for a Software Upgrade and Transformation of Xinjiang Household Registration and Population Information Management System purchased by the Public Security Department of Xinjiang Uyghur Autonomous Region. Examination of Aisino marketing material seems to suggest that Aisino's public security facial comparison management platform is used in Xinjiang.

International involvement

Aisino has sales and service outlets in more than 60 countries. In several of these countries it offers public security traffic management solutions. It also exports biometric data acquisition devices.

Aisino has been instrumental to the development of the Golden Tax Project, which was brought into life in 1994. The Golden Tax Project is intended to modernise the tax system in China. As part of the project Aisino's Golden Tax Division developed Intelligent Tax, a software that banking customers in China must install to pay taxes. In 2020, an American cybersecurity company, Trustwave SpiderLabs revealed that the software came with a built-in backdoor that could allow Chinese authorities access to customers' systems at any time. This incident shows how Aisino's involvement in both the Golden Tax and Golden Shield projects makes it an ideal candidate to provide both the tools to pay taxes digitally as well as to provide the surveillance tools for it. In another twist, Oracle software is used in conjunction with Aisino software in the Golden Tax Project. All businesses in China must use a government-certified tax software for generating Value Added Tax (VAT) calculations and invoices. Oracle is involved by providing Oracle Receivables (an accounting tool) that is then integrated with the Golden Tax Software built by Aisino Corporation.

In 2011, Aisino delivered 80,000 fingerprint acquisition devices to Nigeria for its presidential election to identify voters.

In 2012, Aisino presented its Golden Shield Project solutions overseas to government and non-governmental participants from Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.

In 2015, Aisino showcased its products (e.g. Golden Tax and Shield Project) at the China-Arab States Expo. The question of whether Aisino-produced Golden Tax Software

comes exported with in-built Communist Party backdoors, or whether these are removed for export purposes, remains open for investigation. The China-Arab States Expo was co-hosted by the Chinese Ministry of Commerce, the China Council for the Promotion of International Trade, and the People's Government of Ningxia Hui Autonomous Region.

In June 2016, Aisino held a cooperation symposium with Cisco. Owen Chan, Chairman of the Board and CEO of Cisco Greater China participated in the symposium. The symposium acknowledged the extensive experience Aisino has in government projects and that both parties "are expected to have in-depth cooperation in terms of technology product, project etc…"

Then in 2017, Aisino constructed the National Citizen ID Project for the Republic of Angola, providing products such as card production equipment and ID cards. Those products are central to Aisino's electronic ID card export project.

According to a 2018 IBM Hong Kong Facebook post, Aisino and IBM entered into a business partnership where Aisino will be reselling IBM systems and incorporate them into Aisino solutions. Aisino subsidiary, Huadi, and IBM signed a key business support plan to cooperate in the cloud computing field. Global Vice President Carl Boisvert attended on behalf of IBM. A news article relating to Aisino's Hong Kong subsidiary also speaks of IBM as a project partner.

In 2019, a delegation of the Tajik government met with Aisino's Xinjiang subsidiary and believes that Aisino will engage in Tajikistan's public safety projects.

The subsidiary links section on the Aisino website offers further insight into Aisino's potential activities at home and abroad. SmartTech Production, a company based in Hong Kong, has been linked to Aisino. MIFARE, an integrated circuit products provider, names SmartTech Production as formerly Shenzhen Aisino Takcere Technology Ltd. SmartTech Production has supplied Amsterdam with 1 million public library contactless identity cards. Another affiliate, Aisino Beijing Aerospace Golden Card Banch, has provided permanent resident cards to Xinjiang. Aisino's subsidiary, Aera corporation, is based in San Jose, California.

Neusoft: of Xinjiang and overseas shareholders

Neusoft was founded in 1991 and brands itself as China's first listed software company. In the early 2000s, Neusoft won the bid for a core GSP project. Namely, it assisted in the construction of the Ministry of Public Security's National Basic Population Information Resource Database project. Neusoft's product relating to population management is deployed in Xinjiang by the Xinjiang Autonomous Region authorities and the Xinjiang Construction Corps. The deployed product processes data gathered through the household registration system, fingerprint collection, and facial recognition.

International involvement

The company's website states that it has subsidiaries in the US, Japan, and Europe, and that it was listed four times as one of "Global 100 Software Leaders" by PwC. It cooperates with Intel on network technology and has provided the African Union building in Addis Ababa, Ethiopia with its intelligent venues solutions, which commonly includes visitor behaviour analysis capabilities and emergency centres. Neusoft also has overseas shareholders consisting of Japanese Alpine Electronics, Inc. and German SAP SE.

Neusoft's Romanian-based subsidiary Neusoft European Delivery Center counts Microsoft, Nokia and Philips amongst its partners and clients.

Troila Technology: a surveillance company partners with the World Economic Forum

Troila Technology was established in 2009. The company has been supplying its Police Geographic Information System platform, which falls under the second phase of the Golden Shield Project. Through the platform the police can access maps with information on the police force, buildings of interest and the businesses they contain. Pilot projects of this geographic information system have been launched already during the first phase of the GSP. Beijing, Hangzhou (Zhejiang province), Kunming (Yunnan province), Nanjing (Jiangsu province), Qingdao (Shandong province), and Shenzhen (Guangdong province) were one of the first urban areas to deploy the system.

International Involvement

Troila counts OTIS, an American elevator company amongst its customers and is a partner of the World Economic Forum.

Topsec: of cybersecurity, surveillance, and spying

Topsec is a cybersecurity company that was founded in 1995. Topsec undertook the construction of the Sichuan Provincial Public Security Department's Intranet Network Security Project (2003), part of the larger Golden Shield Project. According to US Embassy cables, PLA officers have been sent to Topsec for network-security training, soon after Topsec was granted access to Microsoft source code. It continues to serve public security authorities by providing website and cloud security products. In 2020 for instance its Next Generation Firewall – which has advanced traffic analysis capabilities – was featured in a bidding document for the Beijing Municipal Public Security Bureau.

International involvement

Topsec mentions that it cooperates with Intel and VMware and that it has implemented cybersecurity projects in ASEAN countries, and Venezuela. Topsec was associated with the 2015 hacking of US insurance company Anthem. The Anthem hack malware matched

closely malware that targeted VAE of Reston, Va., a US defence contractor. The VAE hack was conducted from an IP address associated with the Tianfu hacking competition, which is annually held in China and that Topsec helped organise. More recently, a vulnerability discovered by Qihoo 360, a Chinese cybersecurity company, at the Tianfu competition was allegedly shared with the Chinese intelligence apparatus, who in turn deployed it overnight to spy on the Uyghur ethnic group.

Topsec is part of the Belt and Road Capacity Cooperation Center, which consists of 128 members, amongst them unions, state-owned enterprises, investment agencies, law firms, and individuals that are responsible for fostering China's Belt and Road export strategy. Topsec's role in the Center is to create a cybersecurity platform for the BRI and to supply Chinese companies with cybersecurity products abroad.

The Belt and Road Capacity Cooperation Center

The Center was founded by the Zhongguancun Association of Strategic Emerging Industry, which is an industry promotion platform hailing its name from the Zhongguancun technology hub in Haidan District, Beijing. The Center focuses on commercialising and incubating technology projects. The Center cooperates with partners in 57 countries, including in Spain, where it founded an overseas branch, the UK and Germany. The Centre researches at the same time global corporate competition and organises cultural and business exchanges with countries along the Belt and Road Initiative. In this effort, it established the Advanced Resource Efficiency Research Centre jointly with the University of Sheffield. In turn, Sheffield's partners include Boeing, IBM, Microsoft, Siemens, and Volkswagen, amongst others.

In 2020, the Center also participated in an anti-riot and anti-terrorism forum held at the Ministry of Foreign Affairs and co-organised by the Public Security University. The goal of the forum was to draw attention to the potential of security risks affecting Chinese companies along the BRI routes. Guests included a member of an Israeli counter-terrorism unit.

TRS Information Technology Co., Ltd.: monitoring public opinion for the police and military

TRS is a software company that was founded in 1993. It assists authorities with various public security products. Its opinion monitoring system was used to gauge the public's reaction to the National People's Congress of the People's Republic of China held in 2020. To achieve mass monitoring, it utilises more than 1000 servers. TRS's Info Radar product allows for internet public opinion monitoring by putting in practice dynamic content collection (relates to analysing user behaviour) on websites. What is more, in 2020, TRS signed a strategic cooperation agreement with the People's Public Security University and

established a joint public security opinion laboratory to continue exploring “prediction technology” and to form a unified public security public opinion industry standard. Within the framework of collaboration, TRS provides monitoring training for students at the University. TRS has also been active in working towards military-civil integration, where it aims to promote the application of big data technology in the information military strategy. TRS’s platforms could be used for intelligence, joint warfare and joint training, and counter-terrorism missions.

TRS at a military-civil integration forum in 2016. (Screenshot source)

TRS subsidiary Top Walk was acquired in 2014. In 2019, Top Walk won the bid for a provincial public security information sharing network. The network pertains to the second phase of the GSP and is strongly aimed at integrating data sources from different government departments. Top Walk’s public security products have been used in the Hong Kong-Zhuhai-Macao Bridge and the Zhuhai-Macao travel inspection hall. It developed a Public Security Cloud Search System that classifies more than 300 types of public security industry resources, that relate to people, things, addresses, organizations. Its Public Security Open Source Intelligence Analysis Solution collects and analyses open source intelligence data, creates public opinion warnings so that authorities and businesses can respond in time “to avoid mass incidents”, instability within society, and create a “harmonious network environment.” According to the company, the public opinion warning system works as following: sensitive keywords are set in advance and matched with public opinion information in real time, when negative or sensitive information is discovered, operators are incentivised to conduct a manual review by a series of email reminders, pop-up alarms, and WeChat (instant messenger) reminders. Such a system is used in Heilongjiang province to analyse news sites, forums, and blogs.

International involvement

BMW is a TRS customer, so is Canon. In addition to this, the TRS Internet Financial Risk Early Warning System was demonstrated at the "2014 IBM Cloud Innovation Forum" at the Longemont Hotel Shanghai (previously known as The Regent Shanghai).

Feitian: of the police, the PLA, and Google

Feitian was founded in 1998 and is a Beijing-based supplier of two-factor authentication and smart-card-based products. A 2013 Central Government Procurement Center document shows how Feitian supplied USB keys for the 1203 Project of the Ministry of Public Security, which is a network security subsystem of the GSP. The aim was to gradually equip the national police with USB keys, with a forecasted annual consumption of 700-800,000. It is also likely that Feitian has supplied the People's Liberation Army (PLA), since Feitian's USB Key V2.0 was certified by the PLA's Information Security Evaluation Centre.

International involvement

Google has deployed security keys from Feitian for its Advanced Protection Program. This is a special programme Google offers to people who may be at an increased risk of being targeted online, including human rights activists and journalists, amongst others. Google provides those individuals with additional physical security keys (produced by Feitian), which are required to sign into accounts from a new device and thereby makes it harder for attackers who do not possess this physical key to access user accounts.

On its website, Feitian names Microsoft, Symantec, and Visa as its partners, and J.P. Morgan, SoftBank, UniCredit, Nike as its customers. It has supplied numerous banks, American cybersecurity company FortiNet with its products and names Topsec (see Topsec section) as a long-term trusted partner.

UniStrong: geo-positioning the police and intercontinental ballistic missiles

Beijing-based UniStrong was founded in 1994. It is one of the leading companies in the geo-spatial market. In 2014, UniStrong acquired Changchun Tiancheng Technology Development Co. Ltd., who has been crucially involved in the construction of the GSP. Since the acquisition, Changchun's security products have been integrated into UniStrong. Changchun's main customers are in Xinjiang, amongst them the Xinjiang Public Security Bureau.

It is worth noting that the English language website is almost completely void of content related to military and public security. If one delves into the Chinese language of the website, however, a different picture of the company starts to emerge. The company's core

business – geospatial positioning – is essential to modern police and military operations. As will be laid out below, nowadays police cannot be deployed efficiently if the whereabouts of police officers are unknown, and missiles cannot be launched if state-of-the-art precision technology is not used. This is where UniStrong steps in.

In 2011, UniStrong signed a strategic cooperation agreement with the Institute of Surveying and Mapping of the Information Engineering University of the People's Liberation Army to advance military-civil integration and form a Joint Aerospace Information Research Centre tasked with advanced satellite and UAV (Un[wo]manned Aerial Vehicle) remote sensing. Then in 2018, UniStrong signed a strategic cooperation agreement with the Xinjiang Uyghur Autonomous Region Public Security Department with the aim of establishing a Joint Smart Police Joint Laboratory. The Laboratory is focussed on innovating technologies for large-scale event security, related to emergency command capabilities, and the augmented reality (AR) modelling of crime scenes. UniStrong has several surveillance products that deserve a more in-depth examination.

BeiDou Smart Police Terminal

Its BeiDou smart mobile police terminal integrates functions such as communications features, computer-readable ID card verification, and fingerprint recognition. The mobile terminal can take pictures, scan documents, obtain police data on businesses, buildings, personnel, and vehicles. It has a built-in navigation capability that allows the command center to assess the police force distribution (the positioning accuracy is 3-5 meters).

One of the first large-scale deployments of the mobile terminals was around 2013 to police in Xinjiang, when 20,000 such terminals were delivered to the region. It was also used during the 2014 APEC (Asia-Pacific Economic Cooperation) meeting to enable traffic management during the meeting.

Large-scale event monitoring

The large-scale event monitoring combines drone footage, 3D modelling technology, video surveillance, and the BeiDou navigation and positioning technology. It thereby achieves an efficient resource allocation.

3D modelling of large-scale events for security purposes. (Screenshot source)

Low altitude surveillance

This product deploys radar technology to monitor areas, such as government agencies, borders, and military facilities to prevent illegal photography thereof from UAVs. It thereby has a direct military application.

Community Intelligent Epidemic Prevention and Control Management Platform

This product is used to prevent further spread of the coronavirus but could be used potentially to surveil dissidents. It can control the entry and exit of people, vehicles in monitored areas through facial and vehicle recognition, and perform behaviour, as well as trajectory analysis. It delivers real-name registration and keeps an eye on returnees from other provinces and cities. The product could be used to disperse protests early, since it promises to prevent crowds, queuing, and gathering.

Global Surveying and Mapping Solutions

In June 2015 UniStrong launched this product, which is deployed on the Yuanwang-7 tracking ship. It assures that the ship can achieve a centimeter positioning accuracy. Yuanwang-7 ships are used to track Chinese Army intercontinental ballistic missiles and satellites. In 2020, the product was also used during the launch of the interplanetary mission Tianwen-1.

UniStrong solutions enable the Yuanwang-7 ship to track intercontinental ballistic missiles. (Screenshot source)

International involvement

UniStrong facilities are scattered across the globe, whose locations include Canada, Italy, Japan, Pakistan, Singapore, Thailand, and the US. Its products have been exported to over 90 countries and regions. In 2013, UniStrong acquired Canadian company Hemisphere GNSS. A subsidiary of UniStrong, STONEX is based in Milan, Italy, and has operations all across the world. The controversial nature of the company does not seem to hinder overseas acquisitions. Its RTK product, which provides geospatial positioning services, even won the 2020 German Red Dot Award. The move is controversial since similar UniStrong products were used to conduct measurements on the Chinese-occupied Paracel Islands in the South China sea.

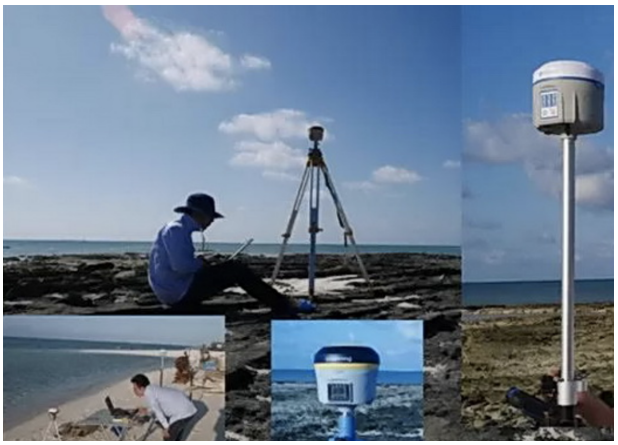
A major aim of UniStrong is to promote BeiDou's global development. UniStrong has participated in the establishment of the China-Arab States BDS Cooperation Forum, the purpose of which is to demonstrate the capabilities of the BeiDou Navigation Satellite System (BDS) to Arab countries and eventually to create a China-Arab Space Silk Road. The aim of the Space Silk Road is to increase bilateral cooperation on modern technologies between China and the Middle East and North Africa.

In 2019, UniStrong participated in an exhibition, which was part of the first China-Central Asia BeiDou Cooperation Forum. Participants came from Cambodia, Indonesia, Kazakhstan, Kyrgyzstan, Laos, Pakistan, Tajikistan, Thailand, Uzbekistan, and Vietnam. UniStrong is co-organiser of the 2020 BeiDou International Training Course. The Training Course is intended to show off UniStrong products and to introduce the BeiDou system to

BRI countries. Representatives from Bhutan, Ethiopia, Kenya, Mongolia, Nepal, Pakistan, Rwanda, and the Thai Embassy in China attended the Training Course.

On a bilateral level, UniStrong helped Pakistan set up a national network, which allows Pakistan to use BeiDou's high-precision services.

More controversially, UniStrong's island and reef mapping products were used in the South China Sea and more particularly on the Paracel Islands. China claims that the Paracel Islands fall under its Sansha prefecture, and has been aggressively militarising the islands. Sansha is a reference to the three disputed geographic features of Macclesfield Bank, the Spratly and Paracel Islands. However, China's claims are highly contested by, amongst others, Vietnam, and the Philippines.



UniStrong's navigation precision products are deployed on Chinese-occupied Paracel Islands. (Screenshot source)

Beijing Zhongke Fuxing Information Technology Co., Ltd.: equipping detention centres in Xinjiang

Zhongke Fuxing was established in 2002 and participated in the general planning and standard elaborations for the GSP. Besides offering a Police Geographic Information System (PGIS), Zhongke Fuxing developed a platform for the Ministry of Public Security to manage one of the eight GSP's databases, the National Information Resource Database of Offenders and Criminals, which is a central data source on all "criminals" within China.

Relatedly, the company developed a Detention Centre Management Information System, which is a software to manage criminal information databases in prisons. The system is intended to be used by the director of the detention centre, management, doctors, and system administrators. It contains detainees' health status and medical records. Zhongke Fuxing created what appears to be an almost identical system for schools – which monitors amongst other things the occurrence of sexually transmitted diseases – and drug rehabilitation centres. In conjunction with this information system, Zhongke Fuxing created a Facial Collection System which is used for capturing images of suspects in detention

centres, and is also compatible with the company's information systems for education centres, and drug rehabilitation centres.

The company states that it completed the following projects in Xinjiang: the Comprehensive Information Management System of Xinjiang Public Security Department Detention Centre, the Comprehensive Information Management System of the Detention Centre of the Public Security Bureau of Xinjiang Construction Corps, and the Digital Monitoring System of Xinjiang Construction Corps.

International involvement

Despite the company's disturbing involvement in Xinjiang, Zhongke Fuxing lists the following companies as its partners:

- Greenplum (a California-based and VMware owned big data technology company)
- IBM
- Intel
- HP
- Microsoft
- Oracle
- SK Inc (one of South Korea's largest conglomerates. It owns SK Telecom)

Xiamen Dragon Information Technology Co., Ltd.: perfecting Uyghur and Tibetan identification tags

Dragon Information Technology has participated in the construction of the first and second phase of the GSP. It is a major provider of public security intelligence platforms.

In November 2017 it signed a strategic cooperation framework agreement with the Tibet Autonomous Region Public Security Department to build the big data and cloud computing for a "safe Tibet" and to create a "stable social atmosphere". In December of that year the Deputy Chief of the Tibet Public Security Department visited the company to learn about its products.

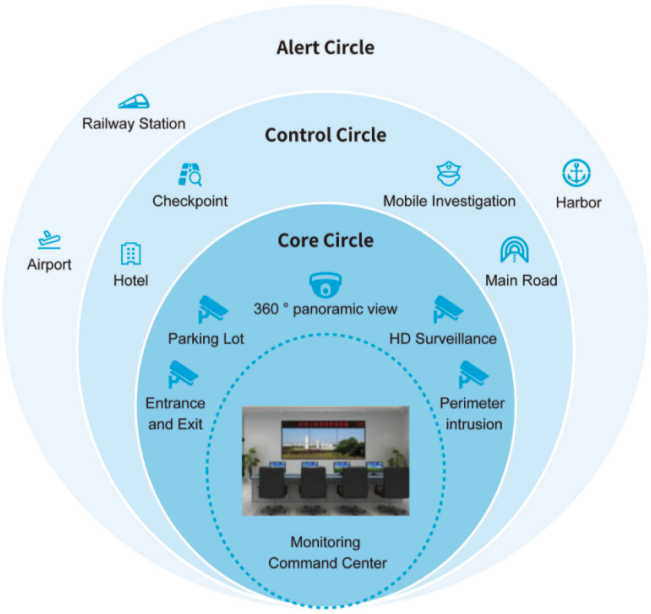
In 2019 it won the bid to expand and upgrade the Ministry of Public Security's Information Sharing and Service Platform (GSP phase II). This platform is currently the main avenue for the Ministry of Public Security to share information with external departments and industry.

In 2021 Dragon Information Technology signed a strategic cooperation framework with the Urumqi Public Security Bureau to advance Urumqi railway public security big data intelligence projects and the smart new police service strategy. Conveniently, Dragon Information Technology has an Urumqi branch.

The company's face capture equipment can collect the MAC address (a phone's unique identifier) and QQ information (instant messaging software) from a passing person's smartphone. Its Video Big Data Platform can scan through 100 million faces in 10 seconds. Dragon Information Technology's Tag Insight System allows police to attribute ethnic labels/tags, such as Uyghur, Han and, Tibetan, to a subject and consequently automatically discover a group of such individuals through these tags. The company's File Cube associates all information on a subject (family, bank cards, whereabouts, property) in one application. Dragon Information Technology's Synthetic Combat Platform enables anti-riot handling. Dragon Information Technology's public security applications are fully compatible with Huawei and Alibaba database platforms

Dragon Information Technology has pioneered a concept of three concentric circles in modern policing. The core is where the event takes place. The control circle encompasses the city. Alarm circle pertains to the exit and entry points into the city, whether these are airports or ports. The idea is to establish concentric circles of policing, where an undesired person would have to cross all circles to attend the event. This could be applied to everyday scenarios where a dissident would be picked up at the airport, and if not there, then at a security checkpoint. The idea behind the concept is that there is one platform that allows one to control all three physical circles through a combination of video analysis and a big data database of citizens, criminals, and political dissidents.

Screenshot taken from video on Dragon Information Technology's website. Concept of policing in concentric circles applied to a city. (Screenshot source)



Dragon Information Technology's concept of policing through concentric circles. (Screenshot source)

International involvement

Dragon Information Technology's international partners are Cisco, Dell, HP, IBM, Microsoft, and Oracle. Its face capture equipment uses the Intel XEON dual 6-core processor. The platform component for the company's Video Big Data Platform seems to use Greenplum products (a California-based and VMware owned big data technology company).

Interestingly, the products that are being advertised for export mirror the GSP databases (fugitives, entry-exit of people, basic data) abroad. This may indicate that the GSP's database standards are diffusing internationally through the export of technology.

From a promotion video it appears that Dragon Information Technology's products have been exported to Abu Dhabi. Dragon Information Technology supports GCC (Gulf Cooperation Council) national license plate recognition. Dragon Information is a leading supplier for Huawei's public security industry products. In its export endeavours, too, it works closely with Huawei, with which it jointly developed a video security solution for major events and a smart police big data solution.

Haiyi Software: integrating information to allow for 24/7 monitoring capability

Haiyi Software company was founded in 2003 and is headquartered in Yantai City, Shandong province. It has participated in both the first and second phases of the GSP. It provides products to public security bureaus across China, amongst them an Urban Multi-Dimensional Perception Monitoring Platform, which integrates existing data from Internet of Things (IoT) devices and social networks to achieve a 24/7 monitoring capability.

Its website proudly presents the efforts Haiyi Software has undertaken to strengthen the ideas and influence of the Chinese Communist Party within the company.

International involvement

Its partners are:

- Accenture
- HP
- IBM
- Microsoft
- Oracle
- SAP SE

Haiyi participated, labelled as a partner, at a 2016 IBM conference on cloud platforms.

Huawei: standing tall amongst China's surveillance giants

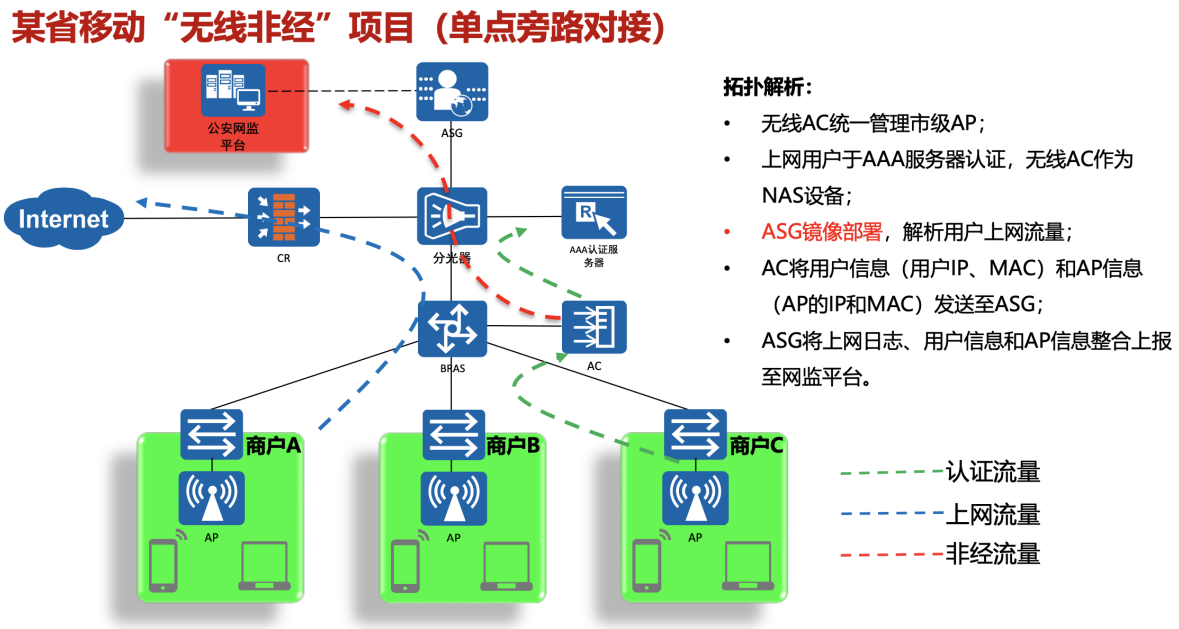
Huawei is a global information technology company and was founded in 1987. The company is part of the first and second phases of the project, as well as its latest development, safe cities.

ASG5000 series surveillance middlebox

Huawei ASG5000 series is an online behaviour management product, which comes with Deep Packet Inspection (DPI) capabilities (an advanced filtering method deployed, amongst others, by the Great Firewall of China to monitor and censor content).

Huawei states that the ASG5000 devices operate in accordance with the Provisions on Technical Measures for Internet Security Protection issued in 2006 by the Ministry of Public Security. The Provisions require ISPs to retain user data, including IP address/domain name, account number, user login and logout time. ASG5000 can determine the user's online identity (e.g., QQ, WeChat, Taobao [online shopping platform] accounts) and track the user's online behaviour (posting content and social network messages).

The ASG5000 middlebox also assists non-ISPs, such as shopping malls and hotels that provide rather than operate internet services to monitor traffic. This necessity is given by the Ministry of Public Security's "Wireless Internet Access Security Technical Requirements for Wireless Internet Access Security Management System in Public Places".

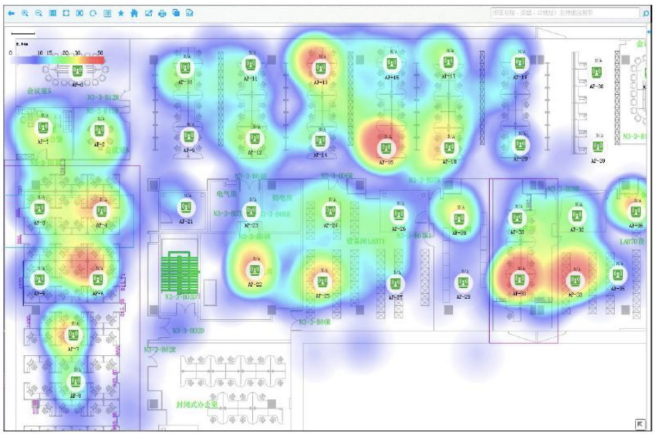


A Chinese province's mobile wireless network. The ASG5000 devices mirror traffic for public security purposes. (Screenshot source)

eSight: Huawei's platform for surveillance and censorship

According to NetEase, a Chinese internet technology company, Huawei's eSight was launched in 2011 at the Singapore Telecom Show. In a Huawei document related to public safety, and that refers to eSight, the company lists IBM, Thales, and Oracle as international partners. The eSight system offers a unified platform for operation and maintenance personnel that encompasses the monitoring of everything from video surveillance to data and cloud centres. Quick fault location in the camera network is promoted as being able to reduce the cost of surveillance.

The system detects faulty devices, their availability, and abnormalities in network flows. eSight recognises traffic from application software, including Yahoo Messenger, BitTorrent, QQ and MSN. Huawei's eSight platform allows for network management on a large scale, which is needed to operate the centralised operation and maintenance of government private video networks. Therefore, eSight products are central to the latest stage of the GSP, safe cities. eSight's WLAN Location Technology uses Bluetooth and Wi-Fi location technologies to track the distribution of e.g., customers in shopping malls. It can create heat maps to see whether people concentrate in certain areas and if this is unwanted, security personnel can "disperse customers or maintain order in a timely manner."



An eSight location heat map of customers in a shopping mall. (Screenshot source)

Use cases are the Gansu Provincial Public Security Department, where Huawei is tasked with updating the information network with the eSight network management platform and in Pingxiang city, in Jiangxi province where eSight is used to operate a police cloud. The Tianjin Public Security Bureau uses it for its Big Data project.

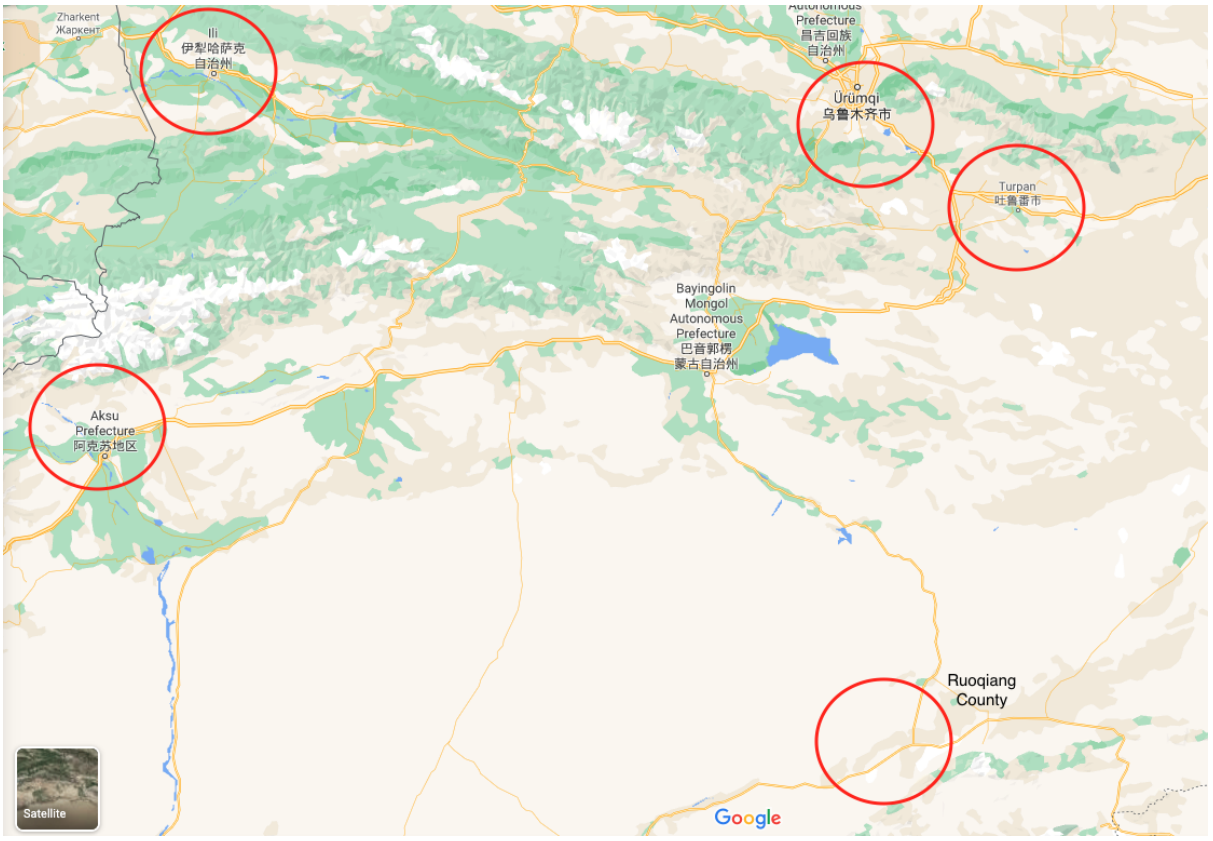
Huawei in Xinjiang

In a Huawei document that appears to be no older than 2013, the company reveals that 80,000 of its cameras are deployed in Xinjiang, covering 90% of the region. 320 sets of Huawei OceanStor 2600T storage products are also present in 9 cities and districts in Xinjiang. According to Huawei, these products "make an important contribution to stability and national security in Xinjiang."

More recently, Huawei's online behaviour management products have been part of a winning contract to supply the company's ASG5300 middlebox to the Diwopu International Airport Branch of the Public Security Bureau of Urumqi City, Xinjiang (2020). Through technical measurement we found two Huawei middleboxes in central Urumqi.[2] eSight is also in use in Turpan, Xinjiang.[3] In addition to this, eSight infrastructure has been deployed to implement online behaviour control at the Xinjiang University College of Science and Technology (Aksu Campus).

Huawei equipment was part of a winning bid to supply the eSight infrastructure to the Ili Prefecture Public Security Bureau (2021) for its public safety video network. Since eSight products are designed for Huawei cameras or mixed-vendor systems it may be that Huawei cameras are used in Ili Prefecture too. Huawei's deep involvement in Xinjiang may also explain why it filed a patent that would allow identifying people of Uyghur origin.

[2] V100R001C00SPC200, China, 87.600456,43.800961, POINT (87.60045599999999 43.800961) and V100R001C00SPC100, China, 87.600456,43.800961, POINT (87.60045599999999 43.800961).
[3] V100R002C02SPC700, China, 89.166672,42.933331, POINT (89.16667200000001 42.933331)



Map 1: Huawei surveillance products in Xinjiang

Unveiling Huawei surveillance middleboxes across the globe

This section describes our investigation into Huawei middleboxes. This research is important, since middleboxes analyse large network flows of sensitive information and are usually placed at key nodes of the internet infrastructure.

Huawei eSight middlebox customers must agree to send extensive amounts of data to Huawei before deploying them, including device name, serial number, model version, and configurations. In addition, customers are encouraged to agree to the devices sending log and performance information to Huawei. This information reveals detailed insights into the ISP and network users within a certain territory. Data from middleboxes outside China is stored in Germany, in Mexico for Latin American customers, and in Moscow for Russian customers. These middleboxes can be found in most networks across the world since they are deployed by most ISPs. Their worldwide dissemination and access to sensitive information means that they are crucial to the national security of any country.

Surveillance middleboxes have a number of applications from firewall and network security (intrusion detection system and intrusion prevention system) to network traffic optimization, asset tracking, and billing. In order to perform these applications most (if not all) middleboxes are implemented in such a way to operate on network traffic or perform a “machine in the middle attack” on the connection that allows them to inspect, manipulate, alter or block parts or the whole network traffic. Given its advanced capabilities, middleboxes have been used for surveillance, distributing malware, tricking users into installing backdoors and rogue software, and to censor network services and websites. Some Huawei middleboxes are available online and can be bought at a cost of $8,000.

A marketing image of Huawei middleboxes found in this report. (Screenshot source)

During research for this report we have detected 1,799 Huawei surveillance middleboxes in 69 countries. We reveal two major findings. First, those devices are used in 17 countries to censor content. Second, they are deployed, with a high likelihood, in 13 countries to run Huawei safe cities. The results of our findings are illustrated on the below map.

Map 2: A global map of Huawei surveillance middleboxes

Huawei middleboxes are used to block websites

During previous research we detected Huawei middleboxes to block websites in 7 countries.

The HTTP header **'Server': 'V2R2C00-IAE/1.0'**, appears to be part of the Huawei product named eSight. Those middleboxes use DPI technology, which is an advanced way of controlling information.

Importance of HTTP headers in detecting surveillance middleboxes

An HTTP header is a mandatory part of web servers and is used by both the client and the server to pass additional information during an HTTP request or response while sending/receiving network traffic to/from websites and network services. An HTTP header provides essentially the metadata of a network traffic connection to the HTTP service protocol.

It is important to mention that middleboxes are often not exposing HTTP headers that reveal their device model and vendor (i.e. the **Server** HTTP header that reveal information about the server software/hardware). This is usually because of their

position on the network; as they may be in specific ISP networks, due to their configuration; a middlebox can be configured to disable some/all HTTP headers. Nonetheless, given the importance HTTP headers have in network traffic, it is very useful to provide all/some HTTP headers so that in case of errors it may be easier to troubleshoot potential issues of the network infrastructure.

Here, we have identified these specific middleboxes to block numerous websites in 17 countries with or without a notification to the user. The categories of the websites that are blocked vary; news/media, hosting and blogging platforms, human rights issues, political/social advocacy, military, alcohol/drugs, pornography, environment, adult/mature content, gambling, religion, art/culture, circumvention tools, internet telephony, news/media, peer-to-peer (p2p), search engines, games, violence/hate/racism, LGBTQI+, business/economy, health, personal/dating, e-commerce and the website youtube.com.

The data analysed is based on network measurements from the following countries: Burundi, Mexico, Afghanistan, Turkey, Bangladesh, Egypt, Spain, Pakistan, Italy, Nigeria, Oman, Paraguay, Colombia, Senegal, Germany and South Africa, during a period of dates from 2017-02-10 to 2021-05-25. The complete results are illustrated in Figure 1 and Figure 2 and in Appendix 'List of blocked websites.'

Cuba

During our analysis we found a number of websites blocked in Cuba by Huawei middleboxes. The majority of blocked websites relate to the categories political and social advocacy, news and media, human rights, censorship circumvention tools, art and culture websites, and websites related to religion and military. In 2017, OONI published extensive research on Internet censorship in Cuba's ParkNets (public Wi-Fi hotspots). Our analysis indicates that since then, the censorship of websites in Cuba has increased. Cuba has only one telecommunications company, ETECSA, which runs the AS27725.[4]

Burundi

In Burundi, we have detected the Huawei middlebox infrastructure to block websites on the networks AS37336, AS327720, AS37429, AS37545, AS25429, AS327799. The blocked websites are associated with Burundi news and media outlets. The blocked websites include radios Inzamba and Isanganiro, the news website Iwacu, and the African Public Radio website.

Afghanistan

In Afghanistan the Huawei middlebox V2R2C00-IAE/1.0 is used to block websites in the AS38742 network that contain gambling and pornography content.

[4] An Autonomous System (AS) is a term that designates a network of internet-connected devices. An AS covers a certain geographical area and is usually operated by a single organisation.

Turkey

Similarly, in Turkey websites in the gambling and pornography categories are blocked. Furthermore, Taraf, a liberal newspaper's website, is not accessible. The newspaper was closed down by decree in 2016, amidst the events surrounding the coup d'état attempt in Turkey, which took place during the same year.

Some of those countries have abysmal human rights records. In Oman, we found LGBTQI+ content blocked, which is in line with the country's criminalisation of homosexuality. In Burundi, we found a domestic radio station to be banned online, which overlaps with the country's persecution of politically dissenting opinions.

In the rest of the countries websites belonging to a wide range of categories are being blocked. This is illustrated in Figure 1 and Figure 2. Although the websites are banned on specific AS networks, we cannot with certainty verify that these websites are subject to country-wide blocking or only local network censorship (e.g., business networks). We can however confirm that these Huawei middleboxes are present on these AS networks and that they are being used to block the enumerated websites.

Country Code / category	AF	BD	BI	CO	CU	DE	EG	ES	IT	MX	NG	OM	PK	PY	SN	TR	ZA	Totals
LGBTQI+	4.5%						8.3%	14.3%					25.0%	25.0%		5.9%		0.2%
adult/mature content	13.6%	16.7%					8.3%			33.3%						5.9%		0.2%
alcohol/drugs	36.4%						8.3%	14.3%		33.3%			8.3%		16.7%			0.4%
art/culture					2.2%			14.3%										1.0%
business/economy					0.4%													0.2%
circumvention tools					2.8%		8.3%							25.0%	16.7%	5.9%		1.4%
e-commerce							8.3%						8.3%					0.1%
environment	4.5%																	0.0%
gambling	18.2%			100.0%		100.0%			100.0%				8.3%	25.0%	16.7%	23.5%		0.4%
games													8.3%					0.0%
health							8.3%											0.0%
hosting and blogging platforms			12.8%		0.1%													6.7%
human rights issues					5.5%													2.5%
internet telephony					1.8%													0.8%
military					2.9%													1.3%
news/media	4.5%	66.7%	87.2%		29.6%		33.3%									11.8%		59.0%
peer-to-peer (p2p)													8.3%		33.3%			0.1%
personals/dating	4.5%						8.3%						8.3%					0.1%
political/social advocacy	4.5%				52.5%						100.0%							23.8%
pornography	9.1%							28.6%		33.3%		100.0%	8.3%		16.7%	47.1%		0.5%
religion					2.2%		8.3%											1.0%
search engines								28.6%					8.3%					0.1%
violence/hate/racism					0.2%								8.3%	25.0%			100.0%	0.2%
youtube.com		16.7%																0.0%
Totals	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Figure 1: Heatmap of blocked websites categories per country (Huawei Middlebox V2R2C00-IAE/1.0')

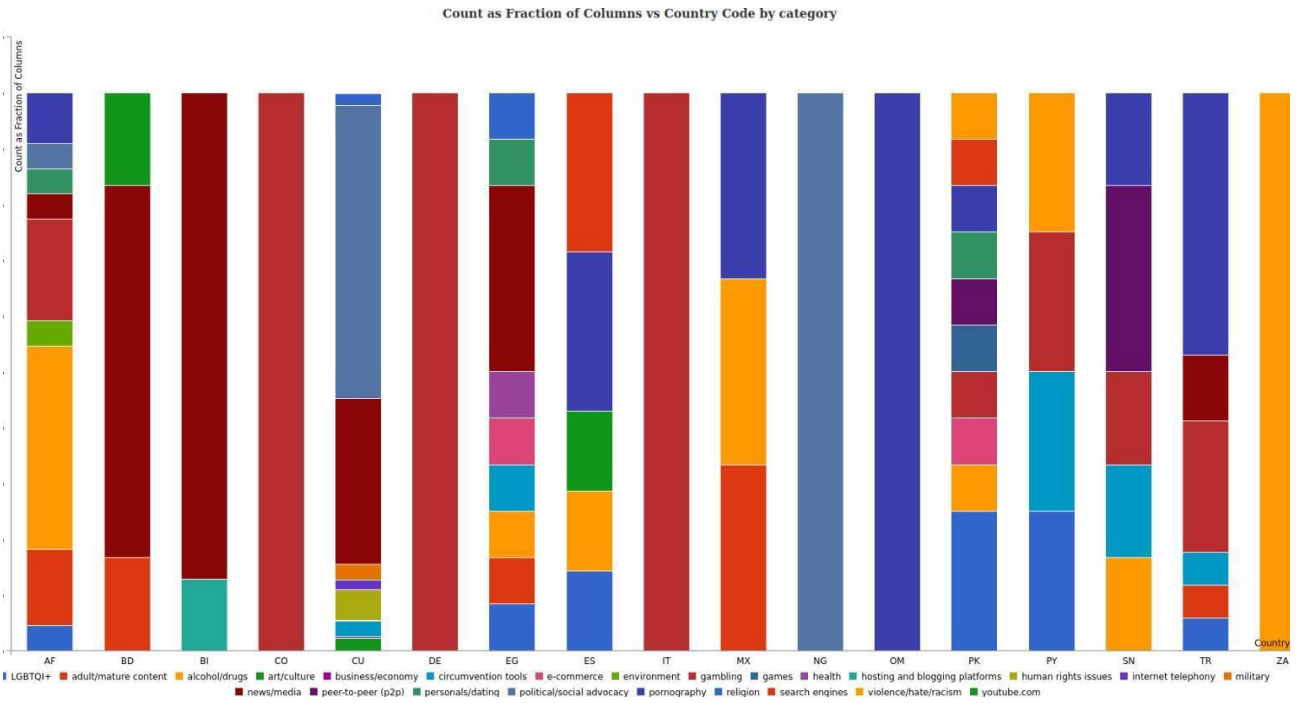
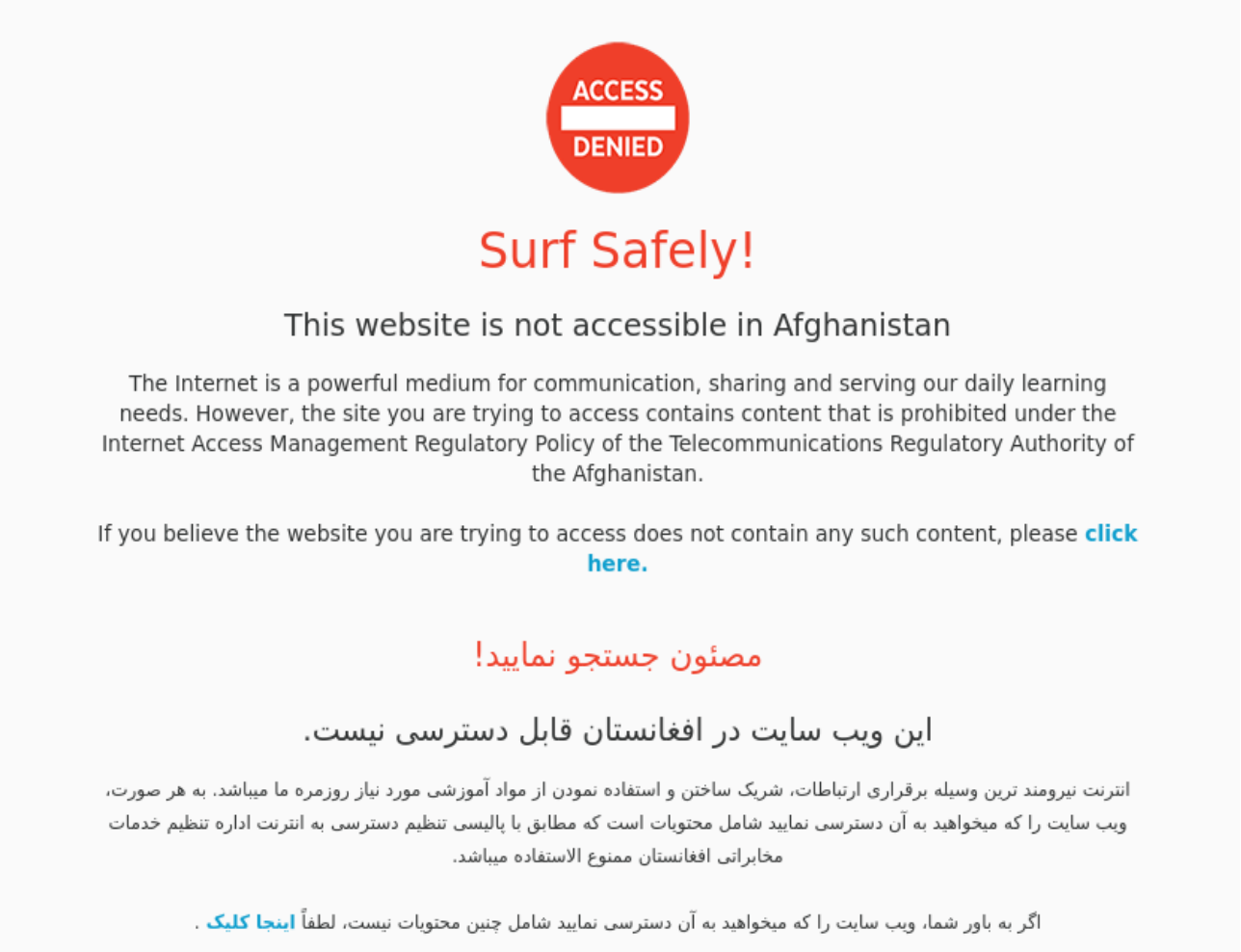


Figure 2: Blocked website categories per country (Huawei middlebox V2R2C00-IAE/1.0')

Blockpage in Burundi - AS327720



Blockpage in Afghanistan - AS38742

Huawei middleboxes are used to run safe cities

Our mapping through technical measurements not only reveals boxes that block online content but also identifies boxes that are likely used to run safe cities. In this report we used the Australian Strategic Policy Institute's "Mapping China's Tech Giants" resource to identify Huawei safe cities. Having identified the geolocations of the safe cities we then cross-examined the location data with the location of middleboxes that we discovered. In this way, we found 13 safe cities that are, according to our findings, at least semi-operational. Those are Caracas (Venezuela), Cochabamba (Bolivia), Dushanbe (Tajikistan), Islamabad (Pakistan), Accra (Ghana), Budapest (Hungary), Johannesburg (South Africa), Kampala (Uganda), Kuwait City (Kuwait), Manila, (Philippines), Nairobi (Kenya), Prague (Czechia), and Singapore.

Our measurements help to add an additional layer of verification to the question if the safe city projects are already operational. Around the world media reports are scarce on information about safe cities. Hence it is often unknown whether they are already in operation. In Uganda for instance the plan is to roll out Huawei safe cities beyond Kampala. Our technical measurements do not yet imply such a roll out has occurred. According to a

Huawei presentation, the company has a safe city presence in Hungary. With the network measurement data, we have a strong indication that the safe city segments in Budapest, Hungary are active and operational.

Recommendations

- We recommend all companies based in liberally minded countries to increase their due diligence of Chinese companies that they receive products from or collaborate with.

- States should increase scrutiny of Chinese owned companies that operate or own subsidiaries on their territory and review whether the companies supply public security bureaus and the military in China.

- Cisco, IBM, and other American companies need to review the third-party contractors that they sell their products to in China and that eventually end up with public security bureaus across the country.

- Countries with Huawei surveillance middlebox presence, that use them for network traffic monitoring or in safe city projects, should curb their use. A massive amount of sensitive information is transiting through these networks daily. As UK intelligence agencies have warned, these products could be potentially used by Chinese intelligence entities for espionage purposes.

Authors

Valentin Weber is a DPhil Candidate in Cyber Security and International Relations at the Centre for Doctoral Training in Cyber Security, University of Oxford. Previously, he was an Open Technology Fund Senior Fellow in Information Controls at the Berkman Klein Center for Internet & Society, Harvard University.

Vasilis Ververis is a PhD candidate at the Humboldt University of Berlin, researching the technical implementations of internet censorship and surveillance. His latest project is the magma guide, an open-licensed, collaborative guide on information controls and internet censorship.

Acknowledgements

We would like to thank Top10VPN for their generous financial support, which made this project possible. We are also grateful to Sam Woodhams and the broader Top10VPN team as well as Dahlia Peterson and PrivacyLx association in Portugal for their valuable feedback. All errors are, of course, our own. Thanks to Madeline Earp at the Committee to Protect

Journalists who identified small typos and discrepancies in a previous version that have since been corrected.

The report was updated on August 17 to adjust Huawei middlebox findings throughout to remove Bulgaria after a small number of geolocation measurement errors in underlying OONI data were identified. These amendments were also applied to the full report, along with correction of minor typos in the "List of blocked websites section" and the addition of a clarifying note in the "OONI data" section.

Ethical considerations

During our research we have neither asked any third parties to perform network measurements nor did we probe any network(s). The complete research and data analysis are based on freely available data and tools without the involvement of any human subjects or personal identifiable information.

Appendix

Data sources

Our research is based on various open and freely available data sources. We have used the Shodan dataset and historical OONI network measurements, a free and open source software that provides the tools and methodology to collect evidence of network interference that may lead to Internet censorship. The data collected on OONI is being submitted by anonymous volunteers from all over the world and is available for use under a creative commons license (CC4.0-BY-NC-SA).

Shodan data

Shodan is a service that offers a search engine and API access to a dataset of servers, network infrastructure and other internet connected devices. We performed numerous queries to discover a multitude of Huawei eSight network infrastructures, we later merged our results with the OONI data to corroborate our findings.

OONI data

We set up an OONI PostgreSQL meta database replica to be able to query all OONI data collected up to October 2020, this helped us to quickly construct specific database queries in order to get all network measurements in the OONI database that present a blockpage based on the Huawei middleboxes. In October 2020 OONI moved to a new data processing pipeline and as a result OONI stopped updating the OONI meta database. In order to overcome this limitation, we used the OONI API. However, we needed to severely decrease the amount of data that we could process and query as it is not anymore feasible to query Terabytes of data without downloading the whole dataset. OONI's data is available under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License.

The total of 1,799 middleboxes specified in this report is based on Shodan data only. OONI data did not contribute to this total as it does not identify individual IP addresses, which means it is not possible to calculate specific numbers of middleboxes. It is however possible to use the OONI data to confirm that there is at least one active middlebox in a particular country.

Mapping China's Tech Giants data

Australian Strategic Policy Institute International Cyber Policy Centre has produced an online database that maps Chinese tech giants' major points of overseas presence. In our research we used the dataset (retrieved in May 2021) to find Huawei's safe city projects across the globe, to then cross-reference the geographic location of the safe cities with the presence of Huawei middleboxes.

Surveillance mapping methodology

We used the Shodan dataset to detect specific Huawei middleboxes. We queried the Shodan dataset for devices that are operating the Huawei Versatile Routing Platform Software, Huawei's own OS. This information has been extracted by fetching the banners of the Simple Network Management Protocol (SNMP) responses. The SNMP protocol provides information about servers or other infrastructure (such as modems, routers, switches) usually connected to a network. The banner fetching helps to extract information on internet connected devices, and the amount of information depends on the (mis)configuration of a specific device. This information is mainly used by administrators to be able to monitor and take asset inventory on devices running on a network.

Below is an example of an SNMP banner captured from one device found in our results. The example provides the OS details such as the version number, device model name, and specific hardware firmware revision as well as the copyright and license information.

```
Huawei Versatile Routing Platform Software
VRP (R) software, Version 8.200 (NE40E V800R012C10SPC300)
```

```
Copyright (C) 2012-2020 Huawei Technologies Co., Ltd.
HUAWEI NE40E-M2K-B
```

Upon collecting all the relevant SNMP banners we have extracted the version and model make of the Huawei devices based on publicly available information.

During the initial iteration of our data analysis we detected that the reported geolocation data of the Huawei middleboxes has been set incorrectly. This is perhaps due to the geolocation database Shodan is using. We were able to correctly geolocate the middleboxes in each country/city by using the IP2Location LITE geolocation database. We were able to construct a map of all the middleboxes found by using the GeoPandas Python library, the results are illustrated in Map 2. We were able to detect 1,799 middleboxes in different regions, countries, cities and 175 unique Huawei middlebox models.

The complete list of device models and versions can be found in Appendix section "List of Huawei middlebox devices in Shodan data."

Network measurement methodology

In this report we measured the presence of middleboxes. According to RFC 3234:

"A middlebox is defined as any intermediary device performing functions other than the normal, standard functions of an IP router on the datagram path between a source host and destination host."

In our research we followed up from a technical report published in 2017 by OONI and a follow-up report from 2019. These reports have detected Huawei middleboxes with the tagged version V2R2C00-IAE/1.0. This version was found to block dozens of websites in Cuba.

For our data analysis purposes we have used free software and open source tools to collect, process, clean, perform exploratory data analysis as well as data visualisation. We used the Python programming language and developed our methodology in iPython Jupyter Notebooks.

List of American companies

Company	Headquarters	Product mentioned in the report	Golden Shield involvement
Cisco	San Jose, California	Netflow Cards	Traffic monitoring

Cognitech Inc.	Pasadena, California	Forensic video analysis	Digital forensics
IBM	Armonk, New York	Servers, Websphere	Police Geographic Information System, Public Security Cloud Platform, Provincial Surveillance Platform
Intel	Santa Clara, California	Core i7 processors, Quad Core processors, Xeon processors	Police Command Centre, Mobile Police Terminal, Provincial Surveillance Platform
Microsoft	Redmond, Washington	Windows 7 OS	Police Geographic Information System, Public Security Cloud Platform, Mobile Police Terminal
Nvidia	Santa Clara, California	GeForce 605 graphics card	Police Command Centre
Oracle	Austin, Texas	Database 10g, 11g	Police Geographic Information System, Public Security Cloud Platform, Provincial Surveillance Platform

List of Chinese companies

Company	Headquarters	Golden Shield involvement	Overseas involvement
Aisino Aerospace Information Corporation	Beijing	Population management databases; emergency platforms; facial comparison management platform	Its tax products are integrated with Oracle software; provided Nigeria with fingerprint acquisition devices; National ID citizen project in Angola; resells IBM systems and cooperates with IBM in the cloud computing field
Beijing Zhongke Fuxing Information	Beijing	Population management databases	Partners are HP, SK Inc (one of South Korea's largest conglomerates. Owns SK Telecom),

Technology Co., Ltd.			Greenplum (a California-based and VMware owned big data technology company), Microsoft, IBM, Intel, Oracle
Bluedon Information Security Technology	Guangzhou, Guangdong	Blocking of anti-censorship tools; Sharp Eyes Project	Strategic cooperation agreement with Dell
DS Communications Equipment Co Ltd	Shanghai	Public security command systems, predictive policing	Collaborates with Huawei to cater to overseas public security market; presence in around 20 countries
Feitian	Beijing	Two-factor authentication products	Supplies Google's Advanced Protection Program, J.P. Morgan, SoftBank, UniCredit, Nike, FortiNet; Partners are Microsoft, Symantec, and Visa
Haiyi Software	Yantai City, Shandong Province	Urban monitoring platform	Partners are IBM, HP, SAP SE, Oracle, Accenture, Microsoft
H3C	Beijing	Emergency command system; public security IP telephone network and data exchange network	Uses Intel processors and memory modules; partners in Canada, Spain, and Portugal
Huawei	Shenzhen	Censorship, safe cities	Global presence. International partners on public safety include IBM, Thales, and Oracle
Neusoft	Shenyang, Lianoning	Population management databases; facial recognition	Subsidiaries in US, Japan, Europe; cooperates with Intel on network technology; Japanese Alpine Electronics, Inc. and German SAP SE are shareholders
Troila Technology	Tianjin	Police Geographic Information System	American OTIS is a customer and Troila is a partner of the World Economic Forum
Topsec	Beijing	Intranet network security for police; traffic monitoring	Cooperates with Intel and VMware; allegedly involved in hacking of US insurance company Anthem; member of Belt and Road Capacity Cooperation Center

TRS Information Technology Co, Ltd	Beijing	Gauging of public opinion; public security information sharing network; cloud search system	BMW is a customer
Unistrong	Beijing	Geo-positioning for police, large-scale event monitoring	Owns Canadian Hemisphere GNSS and Italian STONEX; its products have been used for geo-spatial mapping on disputed Paracel Islands
Xiamen Dragon Information Technology Co., Ltd	Xiamen, Fujian	Public security information sharing and service platform, facial capture equipment	International partners are Oracle, Cisco, Microsoft, IBM, Dell and HP; uses the Intel XEON dual 6-core processor; Video Big Data Platform seems to use Greenplum products

List of Huawei middlebox devices in Shodan data

ACU V200R001C00SPC200
AR120 V200R008C50SPC500
AR120 V200R009C00SPC500
AR120 V300R019C00SPC300
AR1200 V200R008C50SPC500
AR1200 V200R009C00SPC500
AR1220 V200R001C01
AR1220 V200R001C01SPC500
AR1220 V200R002C00SPC100
AR1220 V200R003C01SPC900
AR1220 V200R005C20SPC200
AR1220 V200R005C21
AR1220 V200R007C00SPC900
AR1220-S V200R002C01SPC200
AR1220-S V200R003C01SPC300
AR1220E V200R007C00SPC900
AR1220F V200R007C00SPC900
AR1220W V200R003C01SPC300
AR1220W-S V200R002C01SPC200
AR151 V200R007C00SPC900
AR157 V200R003C01SPCc00
AR157 V200R007C00SPC162T
AR157 V200R007C00SPC900

AR158E V200R003C01SPC900
AR168F V200R007C00SPCb00
AR201 V200R003C01SPC900
AR201 V200R007C00SPC900
AR208E V200R003C01SPC300
AR208E V200R005C20
AR208E V200R005C20SPC200
AR208E V200R007C00SPC900
AR2200 V200R009C00SPC500
AR2200 V200R010C10SPC700
AR2220 V200R001C00SPC500
AR2220 V200R001C01SPC300
AR2220 V200R001C01SPC500
AR2220 V200R002C00SPC200
AR2220 V200R003C01SPC900
AR2220 V200R005C20SPC200
AR2220 V200R007C00SPC600
AR2220 V200R007C00SPC900
AR2220-S V200R002C01SPC200
AR2220-S V200R003C01SPC900
AR2220E V200R007C00SPC900
AR2240 V200R001C00SPC500
AR2240 V200R002C01SPC200
AR2240 V200R003C01SPC300
AR2240 V200R003C01SPC900
AR2240 V200R005C20SPC200
AR2240 V200R007C00SPC900
AR2240-S V200R003C01SPC900
AR2240-S V200R007C00SPC900
AR3260 V200R002C01SPC200
AR3260 V200R003C00SPC200
AR3260 V200R003C01SPC900
AR3260 V200R005C20SPC200
AR650 V300R019C00SPC300
ATN 910C-B V300R002C00SPC100
ATN V200R001C01SPC200
ATN V200R001C02SPC200
ATN V200R006C00SPC100
ATN V200R006C20SPC600
ATN V600R006C00SPC300
CE6810EI V200R001C00SPC700
CE6851HI V200R001C00SPC700
CE6865EI V200R005C00SPC800

CE6865EI V200R005C10SPC800
CX300 V100R002C01B221
CX300 V100R005C02B236
CX600 V600R008C10SPC300
CX600 V600R009C20SPC600
E8000 V300R001C06B035
E8000 V300R001C06B041
Eudemon8080E V100R001C01SPC900
Eudemon8080E V100R003C00SPC200
Eudemon8080E V200R001C01SPC800
Eudemon8160E V200R001C01SPC900
Firewall V200R006C02B066
Firewall V200R007C01B03f
MA5200G V300R003C01B085
MAG9811 V100R001C00SPC100
MAG9811 V100R001C00SPC200
ME60 V600R002C02SPC800
ME60 V600R002C02SPCa00
ME60 V600R007C00SPC300
ME60 V600R008C10SPC300
NE05E-SQ V300R002C10SPC200
NE05E-SR V300R003C10SPC500
NE20-4 V200R005C05SPC100
NE20-8 V200R005C03B383
NE20-8 V200R005C03SPC300
NE20E V200R005C05SPC100
NE20E V800R007C10SPC100
NE20E V800R009C10SPC200
NE20E V800R010C10SPC500
NE20E V800R011C10SPC100
NE40&80 V300R002C01B599
NE40&80 V300R005C01B323SPC001
NE40&NE80 V300R002C01B551
NE40E V800R005C01SPC200
NE40E V800R007C00SPC100
NE40E V800R010C10SPC500
NE40E V800R011C10SPC100
NE40E V800R012C10SPC300
NE40E&80E V300R003C02B608
NE40E&80E V300R003C02B697
NE40E&80E V300R006C01SPC003
NE40E&80E V600R001C00SPC800
NE40E&80E V600R001C00SPCe00

NE40E&80E V600R002C02SPC200
NE40E&80E V600R003C00SPC900
NE40E&80E V600R003C00SPCa00
NE40E&80E V600R007C00SPC300
NE40E&80E V600R008C10SPC300
NetEngine 8000 V800R012C00SPC300
S12700 V200R009C00SPC500
S12700 V200R019C10SPC500
S2300 V100R002C01B070
S2300 V100R002C02B152
S2300 V100R002C02B181SPC001
S2300 V100R003C00SPC301
S2300 V100R005C01
S2300 V100R005C01SPC100
S2700 V100R005C01SPC100
S3300 V100R002C01B070
S3328 V100R002C02B093
S3328 V100R002C02SPC100
S3328 V100R003C00SPC301
S3328 V100R005C01SPC100
S3328 V100R006C03
S3352 V100R002C02B181SPC001
S3352 V100R002C02SPC100
S3352 V100R003C00SPC301
S3352 V100R005C01SPC100
S3700 V100R005C01SPC100
S3700 V100R006C05
S5300 V100R002C02B093
S5300 V100R003C00SPC301
S5300 V100R005C01SPC100
S5300 V100R006C01SPC100
S5300 V200R001C00SPC300
S5300 V200R003C00SPC300
S5300 V200R005C00SPC500
S5700 V100R005C01SPC100
S5700 V200R001C00SPC300
S5700 V200R003C00SPC300
S5700 V200R005C00SPC500
S5710 V200R003C00SPC300
S5720 V200R008C00SPC500
S5720 V200R010C00SPC600
S5720 V200R011C10SPC600
S6720 V200R008C00SPC500

S6720 V200R010C00SPC600
S6720 V200R011C10SPC600
S6720 V200R019C00SPC500
S6730 V200R019C00SPC200
S6730 V200R019C00SPC500
S6730 V200R019C10SPC500
S7700 V200R001C00SPC300
S7700 V200R019C00SPC500
S9300 V100R002C00SPC200
S9300 V100R003C00SPC200
S9300 V100R006C00SPC800
S9300 V200R001C00SPC300
S9300 V200R007C00SPC500
S9300 V200R008C00SPC500
S9300 V200R010C00SPC600
S9300 V200R011C10SPC600
S9300 V200R019C10SPC500
SBC V200R005C02B047
SBC V200R005C02B066
SBC V200R005C02SPC300
SBC V200R005C03SPC400
SVN3000 V100R002C02SPC800
SVN5560V200R001C01

List of blocked websites

In our data analysis we detected numerous blocked websites in various categories in many countries we summarize our results as following:

Country	Category	Domain
Afghanistan	LGBTQI+	['gaytoday.com']
Afghanistan	adult/mature content	['speeddater.co.uk' 'wetplace.com']
Afghanistan	alcohol/drugs	['howtogrowmarijuana.com' 'realbeer.com' 'barmeister.com' 'absinth.com' 'cannaweed.com' 'marijuana.nl' 'dextroverse.org']
Afghanistan	environment	['peta.xxx']
Afghanistan	gambling	['spinpalace.com' 'partypoker.com' 'pokerstars.com' 'poker.com']

Afghanistan	news/media	['towleroad.com']
Afghanistan	personals/dating	['onlinedating.com']
Afghanistan	political/social advocacy	['glaad.org']
Afghanistan	pornography	['bravotube.net' 'hustler.com']
Bangladesh	adult/mature content	['playboy.com']
Bangladesh	news/media	['gazwah.net']
Bangladesh	news/media	['asiantribune.com' 'bnpnews24.com']
Bangladesh	youtube.com	['youtube.com']
Burundi	hosting and blogging platforms	['free.fr']
Burundi	news/media	['rpa.bi' 'isanganiro.org' 'inzamba.org' 'iwacu-burundi.org' 'bujumbura.be' 'ikiriho.org' 'burundinews.free.fr']
Colombia	gambling	['eurogrand.com']
Cuba	art/culture	['vitral.org']
Cuba	business/economy	['cubadata.com']
Cuba	circumvention tools	['tu-dresden.de' 'anonymouse.org' 'inetprivacy.com' 'megaproxy.com' 'anonymizer.com' 'anon.inf.tu-dresden.de']
Cuba	hosting and blogging platforms	['tinyurl.com']
Cuba	human rights issues	['hispanocubana.org' 'sigloxxi.org' 'freedomhouse.org']
Cuba	internet telephony	['pc2call.com' 'callserve.com' 'vonage.com' 'magicjack.com']
Cuba	military	['alpha66.org']
Cuba	news/media	['payolibre.com' 'cafefuerte.com' 'miscelaneasdecuba.net' 'diariodecuba.com' 'cartadecuba.org' 'cubafreepress.org' 'cubamatinal.com' 'cubalibredigital.com' 'cubanuestra.nu' 'cubaencuentro.com' 'voanews.com' 'cibercuba.com' '14ymedio.com' 'martinoticias.com' 'cubanet.org' 'adncuba.com']

Cuba	political/social advocacy	['lanuevacuba.com' 'netforcuba.org' 'nuevoaccion.com' 'solidaridadconcuba.com' 'therealcuba.com' 'conexioncubana.net' 'cubanology.com' 'hermanos.org' 'agendacuba.org' 'asambleasociedadcivilcuba.info' 'cubacenter.org' 'cubademocraciayvida.org' 'cubaeuropa.com' 'damasdeblanco.com' 'directorio.org' 'represorescubanos.com' 'canf.org' 'cubasindical.org' 'cubaliberal.org' 'pscuba.org' 'corriente.org' 'somosmascuba.com' 'avaaz.org']
Cuba	religion	['idealpress.com']
Cuba	violence/hate/racism	['stormfront.org']
Egypt	LGBTQI+	['gay.com']
Egypt	adult/mature content	['flirtylingerie.com']
Egypt	alcohol/drugs	['drugs-forum.com']
Egypt	circumvention tools	['premiumproxy.net']
Egypt	e-commerce	['venus.com']
Egypt	health	['aidsalliance.org']
Egypt	news/media	['wataninet.com' 'koorabia.com' 'korabia.com' 'elbadil.net']
Egypt	personals/dating	['friendster.com']
Egypt	religion	['islamonline.net']
Germany	gambling	['usacasino.com']
Italy	gambling	['pokerstars.net' 'partypoker.com' 'pokerstars.com']
Mexico	adult/mature content	['adultfriendfinder.com']
Mexico	alcohol/drugs	['howtogrowmarijuana.com']
Mexico	pornography	['pornhub.com']
Nigeria	political/social advocacy	['freennamdikanu.com']
Oman	pornography	['gotgayporn.com']
Pakistan	LGBTQI+	['instinctmagazine.com' 'tsroadmap.com' 'thegailygrind.com']
Pakistan	alcohol/drugs	['budweiser.com']

Pakistan	e-commerce	['itunes.com']
Pakistan	gambling	['roulette.sh']
Pakistan	games	['xbox.com']
Pakistan	peer-to-peer (p2p)	['bittorrent.com']
Pakistan	personals/dating	['worldsingles.com']
Pakistan	pornography	['fuckingfreemovies.com']
Pakistan	search engines	['metacrawler.com']
Pakistan	violence/hate/racism	['jewwatch.com']
Paraguay	LGBTQI+	['thegailygrind.com']
Paraguay	circumvention tools	['xroxy.com']
Paraguay	gambling	['gamingday.com']
Paraguay	violence/hate/racism	['whitepower.com']
Senegal	alcohol/drugs	['rollitup.org']
Senegal	circumvention tools	['guardster.com']
Senegal	gambling	['sportingbet.com']
Senegal	peer-to-peer (p2p)	['thepiratebay.org' 'mininova.org']
Senegal	pornography	['hustler.com']
South Africa	violence/hate/racism	['vho.org' 'whitehonor.com']
Spain	LGBTQI+	['transsexual.org']
Spain	alcohol/drugs	['marijuana.com']
Spain	art/culture	['imdb.com']
Spain	pornography	['xvideos.com' 'gotgayporn.com']
Spain	search engines	['google.com']
Turkey	LGBTQI+	['365gay.com']
Turkey	adult/mature content	['89.com']
Turkey	circumvention tools	['anonymouse.org']
Turkey	gambling	['spinpalace.com' 'europacasino.com' 'eurogrand.com']
Turkey	news/media	['halkinsesitv1.org']
Turkey	news/media	['taraf.com.tr']

Turkey	pornography	['alt.com' 'hustler.com' 'infinitetube.com' 'hardsextube.com' 'hotgaylist.com' 'persiankitty.com']