Chairman Mao talked of ‘three magic weapons’ for seizing power: the united front, the armed struggle and construction of the Communist Party itself. Now the priority is remaining in power and to ensure that, the party is developing a fourth ‘magic weapon’.

By combining big data, artificial intelligence, recognition technology and other police techniques, it intends to create a comprehensive method of political and social control. This threatens not only to change Chinese society radically, but also to affect the wider world.

New technology is neither inherently good nor bad. The determinants are human use and restraint. Facial, voice and DNA recognition technology can help in the fight against crime or terrorism. Big data and AI can yield otherwise unobtainable conclusions about tackling diseases and finding cures – an advantage, incidentally, for Chinese medical research, which can draw on the data of a vast population with no privacy limitations – but they might also supply would-be totalitarians with a previously unimagined power to control.

What is this fourth magic weapon?
In the past each Chinese citizen had a dang’an, or file, that covered their life. Nothing could be done without the dang’an. Everything was entered in it – marriage, mobility, job. This new magic weapon may update that surveillance for an infinitely more complex age by tying everything to a person’s unique identifier.

There are five areas making up the magic weapon:
- **Recognition technology** Databases covering the face, voice, fingerprints, DNA of every Chinese citizen.
- **Positional monitoring** Personal mobile devices that report in real time on the location of 1.4 billion citizens; backed up by other public systems, such as the linking up of more than 170 million cameras.
- **Lifestyle monitoring** All databases concerning the individual, be they health or education records, details of purchases made or internet activity, will be monitored. This will include data from the much-discussed Social Credit System, which is like a financial credit rating but which can block those whose behaviour, financial or otherwise, is deemed anti-social, from buying air or train tickets.

A security camera is set up at daybreak overlooking Tiananmen Square before the National People’s Congress in March 2006
The ‘Grid System’ information This divides urban areas into small parcels overseen by citizens who are paid to report unusual activity to the police. Chaoyang district in Beijing, an early experiment, is said to have 120,000 paid informants.

Computer power and AI. To sift through all this information.

What are the Communist Party aims?
As early as 2000, the Golden Shield project aimed to link up all information on all Chinese citizens. At a basic level it would allow authorities to know everything about a particular person within seconds. But it aimed to go beyond that, predicting who might cause trouble to the regime, anticipating the organizing of any action deemed inimical to the party, and curtailing the freedom and actions of any suspect citizen, for example, by taking away the ability to fill up a car with petrol or even in the future to start the engine.

Unsurprisingly, any tool that helps to maintain stability is welcomed by the party. Meng Jianzhu, the head of the security system, hailed big data and modern information technology at a conference in September 2017, talking of ‘extending social governance to the smallest social units, such as villages and communities, in order to realize precise governance’.

His emphasis was on anticipating threats. Earlier in July on a tour of Guiyang province, described by the state news agency Xinhua as ‘a pioneer of the application of big data technology in various sectors, including police work’, he had called on the country’s police to make full use of big data and AI. In August he repeated the message in Xinjiang.

The State Council’s national artificial intelligence development plan declares that, ‘AI is indispensable for the effective maintenance of social stability’.

This is very much in line with the political zeitgeist. Past politiburos were populated by engineers, who saw security solutions in terms of grand projects; the current leadership looks to a new age of ‘informatization’ and IT as aids in governance, and this fits President Xi Jinping’s desire for increased central control.

So, for example, if students are feared as a perennial catalyst for protest, is it surprising that the Ministry of Education has suggested monitoring their political sentiments by collating data from library records, surveys, social media posts and more?

Xi puts great emphasis on ‘law-based governance’ – the Chinese phrase should not be translated ‘rule of law’, because the party is expressly in control of the law. But amid the mass of recent legislation there is little which limits the collection and use of people’s private data; nor, given the importance of maintaining stability for regime survival, are there likely to be safeguards.

‘Law-based governance’ is aimed at controlling the excesses of local government, at making business predictable. There is no intention to limit the party centre’s ability to control the people and rein in dissidents. Xi has committed to increasing political ideology in all aspects of society. Returning to the student example, this new weapon could be used to decide who are eligible for jobs in state-run organizations and businesses.

Appeals against inaccurate information or unwarranted conclusions drawn from it are unlikely to succeed. Good luck to anyone applying under the State Council regulations on open government information. Moreover, the misuse or leaking of material held by the security authorities is not unknown.

What is the progress so far?
In China governance proceeds methodically: plans, pilot projects, lessons learnt and finally schemes extended nationwide.

In a 2017 report on police use of big data systems in China, Human Rights Watch documented a number of experimental zones. Anhui province is building a voice-recognition database. And in the Xinjiang region, where China is engaged in the repression of the minority Uyghurs, much money and effort is being spent combining elements of the new magic weapon. For example, petrol stations allow cars to be filled only through facial recognition linked to ID cards. In addition, all Uyghurs must download an app that automatically reports their browsing of undesirable sites, as well as giving their location.

By researching provincial tender documents, Human Rights Watch has shown that the Ministry of Public Security is pushing ahead with the creation of a ‘Police Cloud’. It notes that: ‘The Police Cloud system appears to be a national project. In 2015, the Ministry of Public Security issued a regulation on information-sharing, ordering aggregation of data and the construction of provincial-level Police Clouds, which form the basis of a
national Police Cloud database. It aims to integrate different types of information, ... such as residential addresses, family relations, birth control methods and religious affiliations ... hotel, flight and train records, biometrics, CCTV footage, and information from other government departments and even private companies.

‘The big data system [can find out] who “has gone to internet cafes together more than twice, or has travelled together twice” with persons of interest.’

In one city, Human Rights Watch discovered that the Police Cloud aims to integrate 63 types of police data and 115 types of data from 43 other government departments and industries. In another, Linyi, whose population is more than two million, the Legal Daily newspaper says there are more than 360,000 cameras. The scale of data collection is heroic.

These are still early days, although examples of arrests through technology are multiplying and the Supreme Court has announced that 6.7 million people have been banned from buying air and train tickets. But there remains a long way to go in development.

Will it actually work?

Can the five elements be united into a totalitarian straitjacket? Three constituencies are important: government, business and public. Government will and funds are there. Chinese business is keen and profiting from it. Human Rights Watch notes that one Xinjiang-based company which integrates AI into its security services saw earnings grow by 260 per cent in one quarter of 2017. Companies are using the region to test big data and surveillance technology and have set up research centres there. Even for companies worried about the principle or about their proprietary information, it makes bad business sense to resist the authorities’ requests to make information held in their databases available.

Meanwhile, the public puts convenience above worries: most areas of life can now be conducted on mobile phones, and few people appear yet to worry about the power this mass of information hands to the authorities.

A very considerable amount of hardware needs to be linked up, to say nothing of the difficulty of ensuring a smooth flow of information from all quarters into the system. Chinese ministries have not been good at exchanging information. The old ministries of water resources and environment never managed a daily exchange of data. Anyone who has worked in government knows the difficulty of setting up, managing and maintaining IT systems.

Another question is whether China can afford the costs. Beyond the computing development and equipment, there are the costs of recognition-system hardware, of the personnel to run and maintain the system, of the payments to the grid system volunteers. If Beijing’s Chaoyang district does have 120,000 volunteers, paid 300 yuan a month, that equates to £50 million a year; copied nationwide, that is an enormous sum.

Quantum computing, with its potential of being millions of times faster than conventional computers, may be key. Its development has become a top priority. But even if the ‘fourth magic weapon’ is not a total success, it looks set to give the party a surveillance machine far more capable and fearsome than it now enjoys.

Might it be counterproductive for the party?

The new system may further erode the trust between people and party. The balance between accepting a convenient electronic life in exchange for personal information and control may tilt. The party is building a considerable constituency of ordinary, non-dissident people who cannot travel or book hotels without being subject to over-frequent checks.

Party members, too, might be unhappy at what is being filed away about them. Interesting questions arise: at what level of seniority do officials cease to have all their personal doings and sayings recorded? Ever? How does the magic weapon play out in factional struggles? Will the security apparatus again have too much power, as it did under Zhou Yongkang, the law enforcement chief who was convicted of corruption in 2014?

And might not innovation, declared essential for China’s future development, be adversely affected, with too much funding being diverted into stability maintenance and because top scientists, businessmen and others might not want to live in such a controlled society? Will those who are talented and wealthier prefer to emigrate, voting in the only way allowed them, with their feet?

How will it affect foreign interests?

The answer is, greatly. Foreign governments need to prepare their responses.

First, the magic weapon will bring enormous changes to Chinese society and behaviour. The need to understand those changes and their effects within and without China will be pressing.

The system may not have foreigners and foreign companies in China as priority targets, but their information will be included. This may even apply to tourists. Moreover foreigners in their own countries and Chinese abroad are likely to be surveilled to some degree. You have to be very trusting to suppose that Huawei or other Chinese companies will not accede, albeit quietly, to party demands for information.

Might the magic weapon be used in trade relations? Big data and AI might enable China to refine its punishment for perceived anti-Chinese stances by other nations by seeking the best way to inconvenience companies or their executives, with minimum harm to China’s own interests.

Meanwhile, foreign companies will have to be more careful to ensure that they do not export to China ‘dual-use’ technology that can be harnessed to surveillance and control systems. Some are already helping development.

Finally, other countries are already expressing an interest in developments; the impetus for Chinese companies to export elements of the system is proving irresistible. Pakistan is at the forefront.

Battle of values

It is fashionable, if perhaps inappropriate as a metaphor in a Chinese context, to conclude that the jury is out. In this case it is not. The ‘fourth magic weapon’ is being built. It may not live completely up to party intentions, but it will affect — is already affecting — Chinese society and human rights more profoundly than any other reform or development instituted by the party.

Already there is a battle of values shaping up between western liberal democracies and a new authoritarianism. This new system of control and repression will accentuate that battle. President Xi Jinping talks of a ‘community with shared future for mankind’. A quarter of mankind looks set to share its future in every detail with the party.

Charles Parton is an associate fellow at the Royal United Services Institute and specialist adviser on China to the House of Commons Foreign Affairs Committee