One internet, two systems. Which will win out after the pandemic?

The Dragon and the Net

Even without the coronavirus, relations between the United States and the People's Republic of China would be strained these days. But the charges that the **Chinese withheld crucial information** before the pandemic broke out has brought the contrast between the nations into sharp relief.

The determined way the East wields the internet to fight the virus provides a sobering view of the net's potential for social control on all levels. It should greatly temper any complacency towards the messy chaos of the West. Yet in many ways, the authoritarian government-controlled internet of 21st Century China is like a dystopian reflection of the anarchical business-controlled net of America.

As the superpowers are geopolitical competitors, so too are their visions of the internet. Out of this rivalry, the online world to come will be made. It might well be built on the Chinese model, one very attractive to authoritarian regimes of all flavors.

The Great Firewall and the Golden Shield

China relies on the same technologies as the West, but it uses them differently. This is due to the long historical isolation that made their language and way of writing so unique. The Chinese call their nation the "**Middle Kingdom**" because they have always seen themselves as the civilized heart of the world surrounded on all sides by jealous barbarians.

As their ancestors built a Great Wall to keep the hordes out, so the modern Chinese have constructed what is called by critics the "**Great Firewall**". This is an array of legal and technical means to monitor, control, and basically restrict internet access with the outside world, to **avoid letting "flies"** be blown in.

Forbidden ideas and censored content include any criticism of the central government or the Communist Party, any mention of the **Tiananmen Square Massacre** or positive talk of democracy, particularly in **Hong Kong**. Lately, anything sounding like **criticism** of the handling of the coronavirus has been added to the list.

Those who seek information on banned topics may be blocked outright, see cleaned-up search results, or links to foreign sites might be slowed until they simply time out. There are **many ways** to deny access, but much interest in evading government restrictions, too. So the authorities use everything from fake websites to trap visitors to tools to spot VPNs tunneling through the Great Firewall.

They can even attack if they want. Special servers outside the Firewall dubbed the "**Great Cannon**" can launch denial-of-service attacks to flood foreign websites with enough traffic to render them useless.

The Communist Party's extensive employment of **propaganda** naturally extends across the internet. **Censorship** openly dominates all their social media, and people must register under their real names. **Dr. Li Wenliang**, who warned of the virus as it killed him, was reprimanded for doing so by officials. Posting complaints, protests, or sharing info can be risky.

Yet some continue to chance it because the authorities are so sensitive to mass discontent. To fight that, officials often employ the "**50-Cent Army**", an online legion of cheerleaders for the state, so called as each post earns them 50¢. In 2016, they made an estimated *448 million* posts and comments.

Behind the Great Firewall, Chinese cyberspace is the planet's biggest **walled garden**, or possibly **greenhouse**, for within it flourishes giant Party-blessed **tech enterprises**, homegrown knock-offs of Western corporations – everything from Apple and Microsoft to Amazon, Google, and even Facebook.

Each corporation lives only by the continuing goodwill of the Communist Party. This fuels Western suspicions about the telecom giant **Huawei**. Whether their smartphones actually contain spyware is less important than that they could secretly be made to. For any company to work in China means playing by their rules, too. Yet the rewards can be so immense that some firms will do almost anything.

Google came under heavy criticism, largely from its own employees, for building a Chinese-language search engine, "**Dragonfly**" that would satisfy Party demands to censor search results. Despite publicly

shutting the project down last year, employees found that the code is **still being worked on**.

As under the old empire, control begins at the border and is carefully imposed on all levels of society across the land. The modern system is called the "**Golden Shield Project**". It has a vast database that scores every Chinese citizen on several financial and citizenship scales, including use of social media.

These scores are vitally significant as bad ones can be crippling. They may involve credit ratings, so people can be charged different amounts. Those convicted of fraud or other offenses can be denied travel permits and tickets or admission to schools.

China has the most **facial recognition cameras** in the world, and its mass surveillance system uses facial recognition software much like **Amazon**'s. This is integrated into daily life by the Golden Shield infrastructure, too, allowing instantaneous posting of a social offender's face and name on electronic billboards as the person crosses an intersection.

Surveillance and Covid-19

From the beginning of the pandemic, the Chinese efforts to fight it have relied heavily on social surveillance and rating systems. Early on, however, automated systems were strained. Facial recognition was **stumped by masks**, and Golden Shield blacklists could not monitor everywhere at once.

So authorities used everything they could think of, like street cameras to track suspected infection carriers, and towers tracking phones' locations. Even drones were used to issue orders to non-masked pedestrians, and security cameras were installed in houses to enforce the lockdown. An immense army of enforcers was hired all across the nation to make sure citizens left their digital footprints everywhere.

In over 200 cities and expanding countrywide, a **smartphone app** that combines tracking location with health updates in real time, sends data about the person's travel and symptoms to the police. To move about, a departing citizen first scans a location code on the building, and then checks in with Alipay, a popular wallet app on their smartphone.

The person is then given a color code that determines just where he or she can go and do. Green is OK, yellow means no entry to public places or transport, and red is to stay at home quarantined.

Police checkpoints enforce these everywhere, too. Travel to hot spots, contact with an infected person, or reported symptoms can instantly change a person's restrictions without any explanation.

While surveillance has been useful in China due to the virus' ability to spread invisibly, its necessity is due not so much to the pandemic but to the **lack of trust** between the people and their rulers. For example, **South Korea** is **struggling** but avoided a total lockdown of the country by a rigorous program of testing and contact-tracing. People understood and believed in what the government was doing.

Yet even better results were in **Vietnam**, which has suffered only one fatality so far. Not only were they prepared and acted fast, they were quite ruthless in quarantining suspected infections and using even more intrusive surveillance than in China.

Right now, at least 30 countries are **ramping up surveillance** of their own populations to fight the virus, including the US. To help track the movements of Americans, the mobile ad industry is teaming up with local, state, and federal governments.

Their data is detailed enough to show whether people are complying with stay-at-home orders and how well **social distancing** is working. It could even follow **illegal pool partiers** in the Ozarks or protesters from NYC as they travel around the country. Google's sharing a trove of map info, too.

Apple and Google are also **developing apps** to notify users of contact with a person who has tested positive. They are quick to note that this is all completely voluntary. The programs that track movement also use location data from apps that have permission to log a person's coordinates.

But is all that **enough**? The coronavirus has demonstrated a remarkable ability to spread without detection. Public health decisions need hard data, even **mass surveillance**, to avoid a second wave.

As the Romans said, "*Necessity knows no law*." If it comes down to a matter of civil liberties or survival, then there is no doubt that freedom will be tossed. The human race will overcome this challenge in any case. The *real* temptations will come afterwards.

Contact-tracing apps could be easily misused especially by **surveillance capitalism**. Governments often try to retain emergency powers once the crisis that required them goes away. The **Patriot Act** was quickly adopted after 9/11 to fight terrorism and is still in effect almost two decades later. Twenty years after Covid-19, will we still be tracked as if infected?