d. The CCP Uses the Masses for Espionage

The CCP regards information as simply another weapon in its arsenal. Regardless of the field, whether pertaining to the state, private enterprise, or individual endeavors, all forms of information are seen as fair game for the fulfillment of the regime's strategic ambitions.

The CCP has also used legislation to force all Chinese people into participating in its unrestricted warfare. The National Intelligence Law of the People's Republic of China, passed by the Standing Committee of the National People's Congress, clearly states that "national intelligence agencies may require relevant agencies, organizations,,and citizens to provide necessary support, assistance and cooperation."[54] This means that any Chinese citizen can be coerced by the CCP to collect intelligence and become a spy. This form of intelligence collection has never been seen before.

On December 12, 2018, the U.S. Senate Judiciary Committee held a hearing about the CCP's "non-traditional espionage activities." Bill Priestap, deputy director of the FBI counterintelligence department, revealed the characteristics of these activities: They sometimes play by the rules when it's to their advantage, while at other times, they bend and break the rules to achieve their goals. When capable, they also try to rewrite the rules and reshape the world according to their own requirements.

John Demers, assistant attorney general of the National Security Division of the U.S. Department of Justice, testified that the CCP's Made in China 2025 plan, while on the surface aimed at improving innovation,

is essentially a handbook for what to steal. He disclosed that from 2011 to 2018, over 90 percent of the cases of economic espionage allegedly involving or benefiting a country were related to China (that is, the CCP), and that over two-thirds of the trade-secret theft cases are connected to China (again, meaning the CCP).[55]

In the previous section, we discussed the CCP's hacking companies and inducing personnel to steal Western intellectual property. In fact, the CCP's espionage is far from limited to intellectual property.

The CCP controls all major private companies in China and uses these nominal "private enterprises" for international intelligence gathering. Ted Cruz, the U.S. senator from Texas, said Huawei was a "Communist Party spy agency thinly veiled as a telecom company." "Its surveillance networks span the globe and its clients are rogue regimes such as Iran, Syria, North Korea, and Cuba. The arrest of Huawei's CFO Wanzhou Meng in Canada is both an opportunity and a challenge," he wrote.[56]

According to a survey released in January 2018 by the French newspaper Le Monde, confidential information from the African Union (AU) headquarters in Ethiopia was sent to Shanghai every night for five years. The CCP was accused of being behind the hack. A report released by the Australian Strategic Policy Institute (ASPI) on July 13 revealed that Huawei is a provider of some network-technology infrastructure at the AU headquarters building.[57]

André Ken Jakobsson, a postdoctoral fellow at the Center for Military Studies in Copenhagen, said: "What is worrying is that the CCP can get very critical and sensitive information. They can enter a system that

controls our entire society. Everything will be connected to the 5G network in the future. We are worried that the country that provides such equipment — China [the CCP] — controls the switch."[58]

In China, the CCP uses cameras, computer networks, and artificial intelligence equipped with face-recognition technology to create a ubiquitous monitoring network. If it is not stopped, the situation prevailing in China today is likely to spread around the world tomorrow.

At the same time, the CCP has used hackers on a large scale. As early as 1999, the CCP's hackers disguised themselves as a Falun Gong overseas website and attacked the U.S. Department of Transportation. The Department contacted the Falun Gong website to clarify the facts. Then the relevant personnel traced back and found that the real hacker came from an intelligence agency run by the Party.[59]

In June 2015, the U.S. federal government was invaded by CCP hackers who stole a large amount of confidential information — the information of more than 21.5 million Americans. Affected people included 19.7 million government employees and 1.8 million family members of these government employees.

In November 2018, Marriott International announced that private information, including passports, of up to 500 million guests was attacked by hackers, dating back to 2014. U.S. Secretary of State Michael Pompeo confirmed on December 12 that the hacking was carried out by the CCP. Marriott is the largest hotel supplier to the U.S. government and military.