



INCLUSIVE SOCIETY INSTITUTE

Op-ed

WHO WATCHES THE SUPERPOWERS WHEN THEIR TECHNOLOGY WATCHES US?

By Daryl Swanepoel

The debate over Chinese technology is framed almost entirely around one question: can Beijing use Chinese-built telecommunications networks, cloud systems, artificial-intelligence platforms or drones to conduct surveillance? The answer is yes. It is technically possible. But stopping there produces a dangerously incomplete picture, because precisely the same question must be asked of the United States.

Modern digital technology is not politically neutral infrastructure. Telecommunications equipment processes traffic and metadata. Cloud providers store information and control access to computing capacity. Drone platforms collect imagery, coordinates and flight histories. AI companies process prompts, documents and organisational data. Manufacturers can alter the behaviour of these systems through software and firmware updates.

Any state able to compel, compromise or cooperate with the companies controlling these technologies may potentially gain access to valuable information. That is true whether the supplier is Chinese or American or any other country for that matter.

Western security concerns about China are not imaginary. Article 7 of China's National Intelligence Law requires organisations and citizens to support, assist and cooperate with national intelligence work. Chinese state-sponsored cyber operations against telecommunications and critical infrastructure have also been documented. A 2025 joint advisory issued by the United States and international partners described Chinese-linked actors compromising networks around the world to support an espionage system.

The technical risks are equally credible. Telecommunications equipment contains remotely maintained software, while internet-connected drones can transfer imagery, location information and telemetry. Joint guidance from the US Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation warns that Chinese-manufactured unmanned aircraft systems can create pathways for data to leave an organisation and that manufacturer-controlled updates could introduce previously unknown collection functions.

These are legitimate reasons for scrutiny. They are not, however, evidence that every Chinese product contains a hidden backdoor or that all data passing through Chinese equipment is automatically delivered to Beijing. British authorities examining Huawei equipment repeatedly identified serious weaknesses in software engineering and security assurance. However, the official 2019 Huawei Cyber Security Evaluation Centre Oversight Board report stated that the identified defects were not believed to be the result of Chinese state interference. Similarly, some technical assessments of Chinese drones have found vulnerabilities, while other controlled tests have detected no unexpected transmission of data.

Capability, vulnerability and proven exploitation are not the same thing.

That distinction becomes even more important when the United States presents the choice as one between risky Chinese technology and trusted American technology. American technology may operate within a more transparent legal and institutional system, but it is not beyond the reach of the American state.

The United States openly conducts foreign electronic surveillance. Section 702 of the Foreign Intelligence Surveillance Act authorises the targeting of non-American persons outside the United States, with the compelled assistance of American electronic communications service providers. According to the US Privacy and Civil Liberties Oversight Board, approximately 349,823 non-US persons abroad were targeted under this authority during 2025.

This is lawful surveillance under American legislation and subject to American oversight. But that does not make it irrelevant to foreigners. The protections available to American citizens are not necessarily extended to foreign governments, companies or individuals whose communications pass through American-controlled services.

The uncomfortable question therefore becomes unavoidable: if China's ability to compel Chinese companies creates an unacceptable espionage risk, why should the American government's ability to compel American companies be treated as benign?

There are differences. The United States has courts, congressional oversight, a more independent media and stronger avenues for challenging government conduct. China's intelligence system is considerably less transparent, and Chinese companies have less visible scope to resist state demands. These distinctions can affect the level of risk. They do not extinguish the underlying risk.

Nor is surveillance the only concern. Technological dependence creates strategic leverage. A foreign power may be able to restrict cloud services, revoke software licences, withhold security updates, interrupt access to advanced chips or prevent equipment from receiving essential support. American export controls already demonstrate how technological dominance can be converted into geopolitical power. China possesses similar potential wherever its infrastructure and platforms become indispensable.

Replacing complete dependence on China with complete dependence on the United States would therefore not produce technological sovereignty. It would transfer the dependence from one superpower to another.

This is why a bilateral US–China AI mechanism, although valuable, cannot provide an adequate global answer. Washington and Beijing are not neutral custodians of the international technological order. They are intelligence powers, commercial competitors, regulators and owners of the dominant technology ecosystems. Each has an incentive to emphasise the dangers presented by the other while seeking wider international adoption of its own systems.

A bilateral agreement may reduce the danger of miscalculation, establish communication channels and help contain AI-enabled cyber incidents. But it cannot legitimately determine the conditions under which the rest of the world must live with American and Chinese technology. At worst, the two powers could manage their rivalry between themselves while leaving other countries as rule-takers within competing technological spheres.

That makes the United Nations Global Dialogue on AI Governance far more important than another diplomatic talking shop. Established by the General Assembly through Resolution 79/325, the dialogue provides a forum in which countries that do not control frontier AI models, global cloud platforms or semiconductor supply chains can participate in shaping the rules.

Its value lies in the possibility of replacing geopolitical trust with universal standards. Those standards should require transparency about remote access, data storage, government requests, firmware updates and cross-border data transfers. Critical systems should be independently auditable. Encryption keys should remain under the control of the country or institution using the technology. Suppliers should disclose vulnerabilities and provide credible offline operating options. No government should obtain covert privileged access merely because a company falls under its jurisdiction.

Most importantly, the same requirements must apply to Chinese, American and other suppliers. Rules that presume American trustworthiness while demanding proof of Chinese innocence will lack international legitimacy. So will Chinese appeals to sovereignty that are not accompanied by verifiable limits on Beijing's access to data held by Chinese companies.

The UN dialogue does not itself enforce such a regime. It is not a treaty body, international inspectorate or global technology regulator. Its value will ultimately depend on whether participating states can move beyond broad ethical declarations and develop practical, reciprocal and independently verifiable assurance standards.

The world does not need Washington to certify American technology or Beijing to certify Chinese technology. It needs common rules under which neither power is simply expected to be trusted.

The real question is no longer whether China can spy through technology. It is who watches all the powers whose technology may be watching us, and whether the rest of the world will have any meaningful say in the answer.

Daryl Swanepoel is the Chief Executive Officer of the Inclusive Society Institute and a Research Fellow at the School of Public Leadership, Stellenbosch University.