DISCUSSION PAPER



Chinese Espionage: A World Menace?

Çağdaş Yüksel

TRT WORLD research centre

DISCUSSION PAPER

Chinese Espionage: A World Menace?

Çağdaş Yüksel

TRT WORLD research centre

© TRT WORLD RESEARCH CENTRE

ALL RIGHTS RESERVED

WRITTEN BY

Çağdaş Yüksel

PUBLISHER

TRT WORLD RESEARCH CENTRE

April 2023

TRT WORLD İSTANBUL

AHMET ADNAN SAYGUN STREET NO:83 34347

ULUS, BEŞİKTAŞ

İSTANBUL / TÜRKİYE

TRT WORLD LONDON

PORTLAND HOUSE

4 GREAT PORTLAND STREET NO:4

LONDON / UNITED KINGDOM

TRT WORLD WASHINGTON D.C.

1819 L STREET NW SUITE 700 20036

WASHINGTON DC

www.trtworld.com

researchcentre.trtworld.com

The opinions expressed in this discussion paper represent the views of the author(s) and do not necessarily reflect the views of the TRT World Research Centre.

Introduction

Allegations of Chinese spying activities have been on the rise in recent years, with numerous countries accusing China of engaging in espionage, cyberattacks, and other covert operations. These allegations have created tensions between China and its allies, as well as countries that have historically been suspicious of China's intentions. These claims suggest China has engaged in various espionage activities, including cyber-attacks and human intelligence operations.

In 2023, the first major tension regarding these accusations started when the United States shot down the 'spy' balloon belonging to China. In February 2023, upon detecting a suspicious balloon moving from China to the United States airspace over Canada, the USA requested information from the Chinese government through the Beijing Embassy. Chinese officials explained the situation as "a civil aircraft used for meteorological activities". US officials rejected China's statement of meteorological activities because the balloon could "manoeuvre". The balloon in question was dropped on February 4, 2023. Following these developments, the visit of US Secretary of State Antony Blinken to Beijing was postponed (Dag, 2023).

After the balloon crisis, claims by the US that China could carry out espionage and sabotage activities with giant cargo cranes at US ports came to the fore. The Wall Street Journal, citing Pentagon officials, stated that China could use giant cargo cranes in US ports for espionage and sabotage. In the news, which stated that some national security and Pentagon officials compared the cranes to a "Trojan horse", it was noted that the cranes contain sensors that can track containers and predict their destination (Viswanatha et al., 2023).

The latest development between the two countries was TikTok CEO Shou Zi Chew's defence in the US Congress against the complaints that his company provided data to China and spied for the benefit of China. Chew suggested that ByteDance, TikTok's parent company, is "not owned or controlled by the Chinese government "(Paul & Bhuiyan, 2023). Apart from the US, allegations of spying activities related to TikTok were also made in Canada, England, Netherlands, France, Denmark, Belgium, Norway, New Zealand, India, and Taiwan. Consequently, several governments took a series of measures regarding this application (Euronews, 2023).

China's intelligence-gathering activities have been source of concern for decades. However, the scope and complexity of these activities have increased in recent years, putting this subject front and centre on the agenda of the international community. China's intelligence-gathering endeavours focus on obtaining military, economic and technological information from foreign countries, and have made waves in recent years.

The Chinese government has consistently denied these accusations, claiming they are baseless and politically motivated. However, the highly mediatised incidents have led to increased tensions between China and the West. This paper discusses the allegations of Chinese espionage activities and their global impact.



(Miguel Candela - Anadolu Agency)

Cyber Espionage

The act of utilising digital technology to get unlawful access to private or sensitive information or data belonging to a person, company, or government agency in order to conduct surveillance or gather intelligence is known as cyber espionage. Governments, corporations, groups, and individuals engage in this type of espionage for various objectives, including political, military, economic, and personal benefits (Weissbrodt, 2013).

The rise of digital technologies has made gathering sensitive information from remote locations easier than ever. This situation has led to an increase in cyber espionage activities around the world. Governments and businesses alike have become targets of cyber espionage, with attackers using sophisticated techniques to infiltrate computer systems and steal sensitive information (Lewis & Baker, 2013). The range of activities range from stealing important intellectual property or financial data to gathering information on political or military rivals. Cyber espionage has become a menace to governments, corporations, and people worldwide because of its covert nature and capacity for plausible deniability (Geers et al., 2014).

China is believed to be focused on stealing sensitive information, including military and defence-related technology, intellectual property, and trade secrets (Lindsay et al., 2015). As a result, Beijing is seen as one of the most potant cyber threats to countries, companies, and organisations worldwide. The Chinese government has been accused of sponsoring and supporting cyber espionage and hacking campaigns targeting governments, military organisations, companies, and academic institutions.

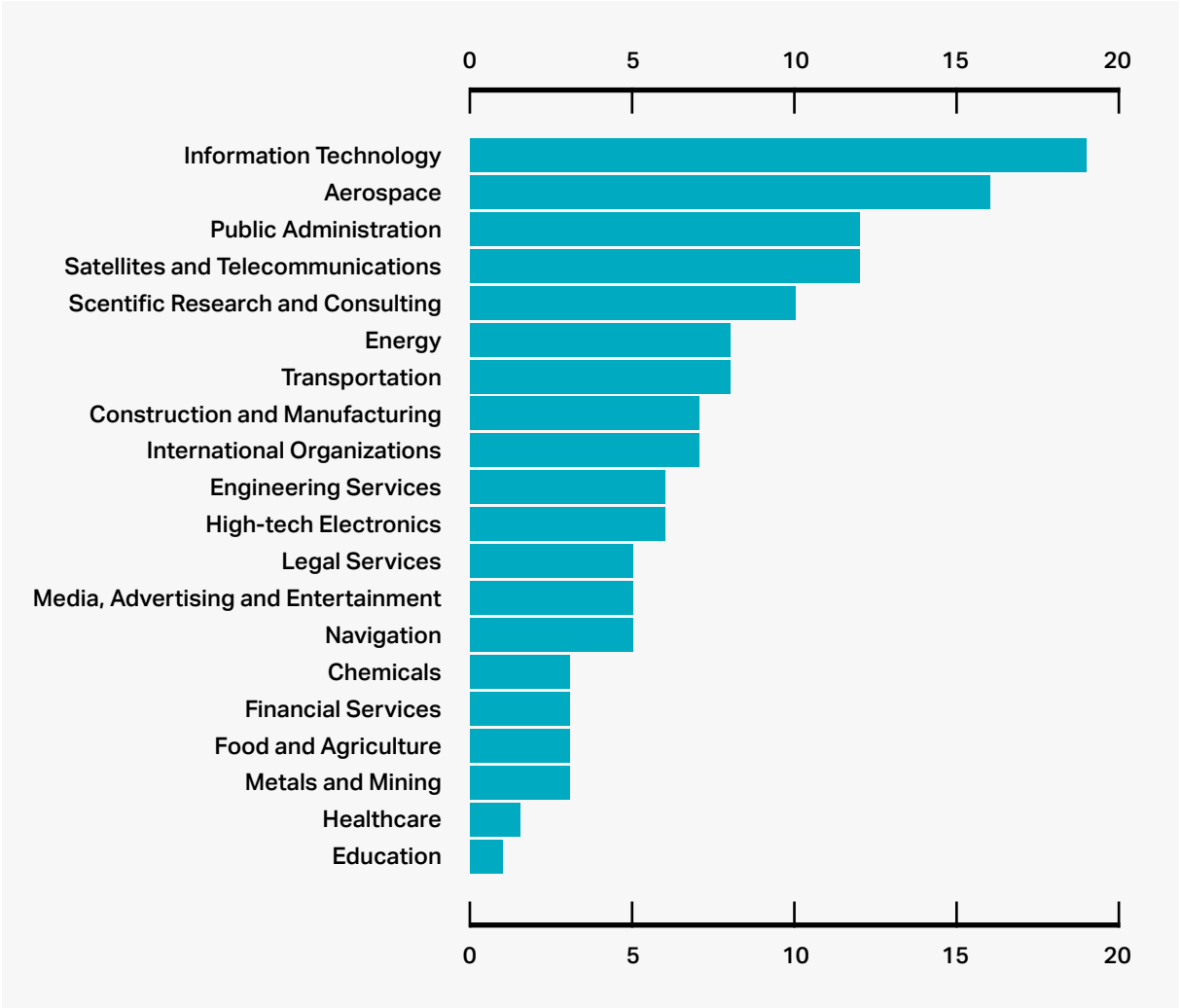
Meanwhile, China is increasing its dependence on new technologies every year by using all the opportunities offered by the internet and information technologies. While the number of people using the internet in China was 564 million in 2012, it reached 1 billion in 2022 (Thomala, 2023). While this situation gives the edge to Beijing on many fronts, it also creates issues, such as the rise in cybercrime. Therefore, cybersecurity has become a priority issue for China.

China emphasises that cybersecurity is important in the national defence system, as expressed in its 2008 Defence Report (Information Office of the State Council of the People's Republic of China, 2009). The 2010 Defence Report underlined that significant investments would be made to develop and strengthen cyberspace (Information Office of the State Council the People's Republic of China, 2011). In addition, in the 2015 report, the country's security areas, such as space, cyberspace and nuclear capacity, were added, and the importance of the subject was clearly emphasised. China has not included such strategic military elements in its defence strategy documents published until 2015 (Gady, 2015).

China's cyber espionage efforts have been associated with several advanced persistent threats (APTs). APT (Advanced Persistent Threat) is a highly prolific hacking group operating outside China. This group, detected and tracked by the security firm Mandiant, has occasionally launched cyberattacks worldwide (Sganga, 2022). According to the report, the Chinese People's Liberation Army (PLA) cyber command is fully institutionalised within the Chinese Communist Party (CCP) and can leverage the resources of China's state-owned enterprises to support its operations. The report also stated that China has a cyber security army with 130,000 personnel divided between 12 bureaus, three research institutes and 16 regional and functional bureaus (Mandiant, 2013). The sectors targeted in the report between 2006 and 2012 are shown as follows (Mandiant, 2013).

In addition to Mandiant's report, countries such as Taiwan, Japan, India, Canada, the UK, and Australia have routinely reported China-related cybersecurity concerns. In a July 2021 joint statement with NATO, the EU, and other Western nations, the US accused China of conducting several cyberattacks, most notably the 2021 Microsoft Exchange Server data breach. A cyberattack on Microsoft's Exchange email servers affected thousands of computers worldwide, allowing attackers to access sensitive information. It was stated that the cyber-attacks on Microsoft aim to track computers belonging to small American businesses, state governments and some military companies with malicious software that secretly tracks their movements (Kanno-Youngs & Sanger, 2021).

US media also reported that in the 2016 and 2018 elections, Chinese hackers attempted to attack electronic election systems, and in the 2020 Presidential elections, these attacks were renewed, and US political figures were targeted before the elections (VOA, 2020).



Is 5G a Security Threat?

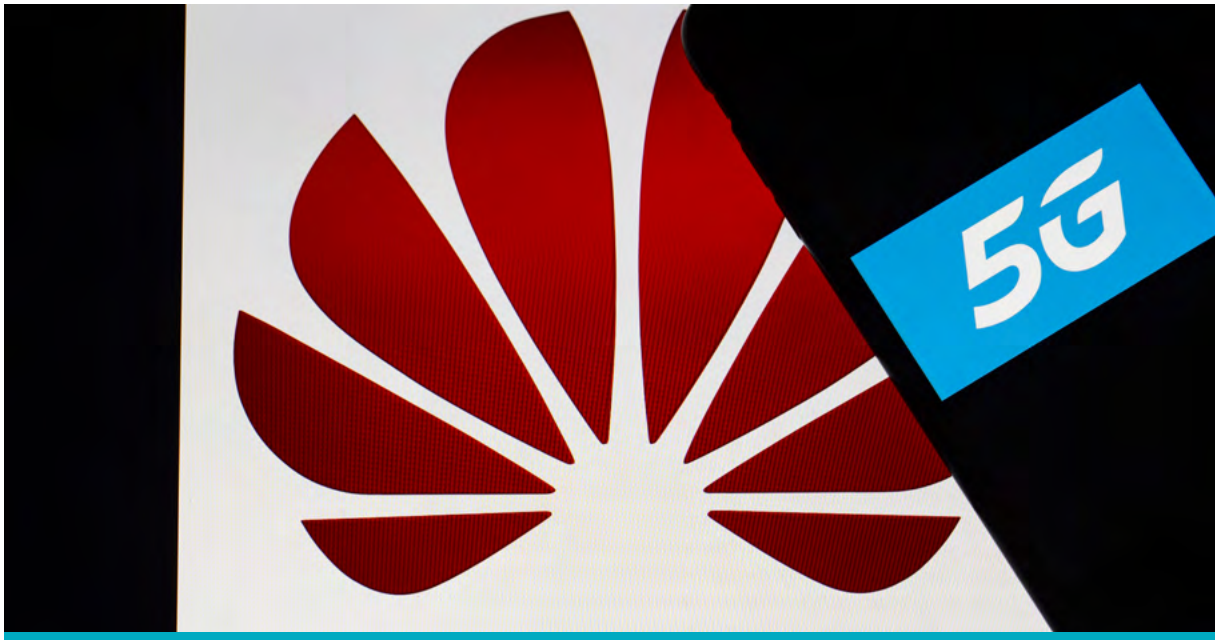
Western public opinion is more sensitive to security threats brought forward by Beijing-owned social media platforms and 5G technology.

The rollout of 5G technology has brought renewed scrutiny to two Chinese firms, Huawei and ZTE, as the companies are one of the leading suppliers of 5G equipment. The US, Canada, New Zeeland, Japan, England, and Taiwan have raised concerns that these companies' technology could be used to spy on governments and businesses. Consequently, authorities moved to restrict or ban the use of Huawei equipment in their 5G networks (Ellsworth, 2022).

One of the main concerns with Huawei and ZTE's 5G technology has been the claim that it could potentially allow the Chinese government to spy on a large scale. 5G networks power critical infrastructure, from smart cities and autonomous vehicles to military communications and medical devices. The massive scale of 5G networks raises concerns that any vulnerabilities in the technology could be exploited by malicious actors, including the Chinese government and criminal organisations (Berman et al., 2023).

The US was tenth in Huawei's warnings about the security risks associated with 5G technology. The Trump administration issued a decree on May 15, 2019, banning US companies from using Huawei and ZTE equipment in 5G networks, citing national security concerns (Brown, 2022). The US government also warned its allies to remove Huawei from their 5G networks, arguing that the company's equipment could be used for spying by the Chinese government.

Additionally, social media platforms of Chinese origin came to the fore when allegations surfaced regarding spying activities. The social media platform TikTok, developed by China-based technology company ByteDance, has reached more than 1 billion users around the world, and has brought accusations of being a "Chinese espionage tool". The biggest reason for the TikTok ban is that TikTok and its parent company ByteDance have given sensitive user data, such as location, to the Chinese government. As a reason for this, it is pointed out that the government in China has the right to request data from companies. The UK, Canada, the European Union (EU) and New Zealand banned the app from governmental devices, while India was the first country to ban TikTok in 2020 (TRT Haber, 2023). Responding to allegations about his company in the US Congress, TikTok CEO Shou Zi Chew denied the allegations about his company (Paul & Bhuiyan, 2023).

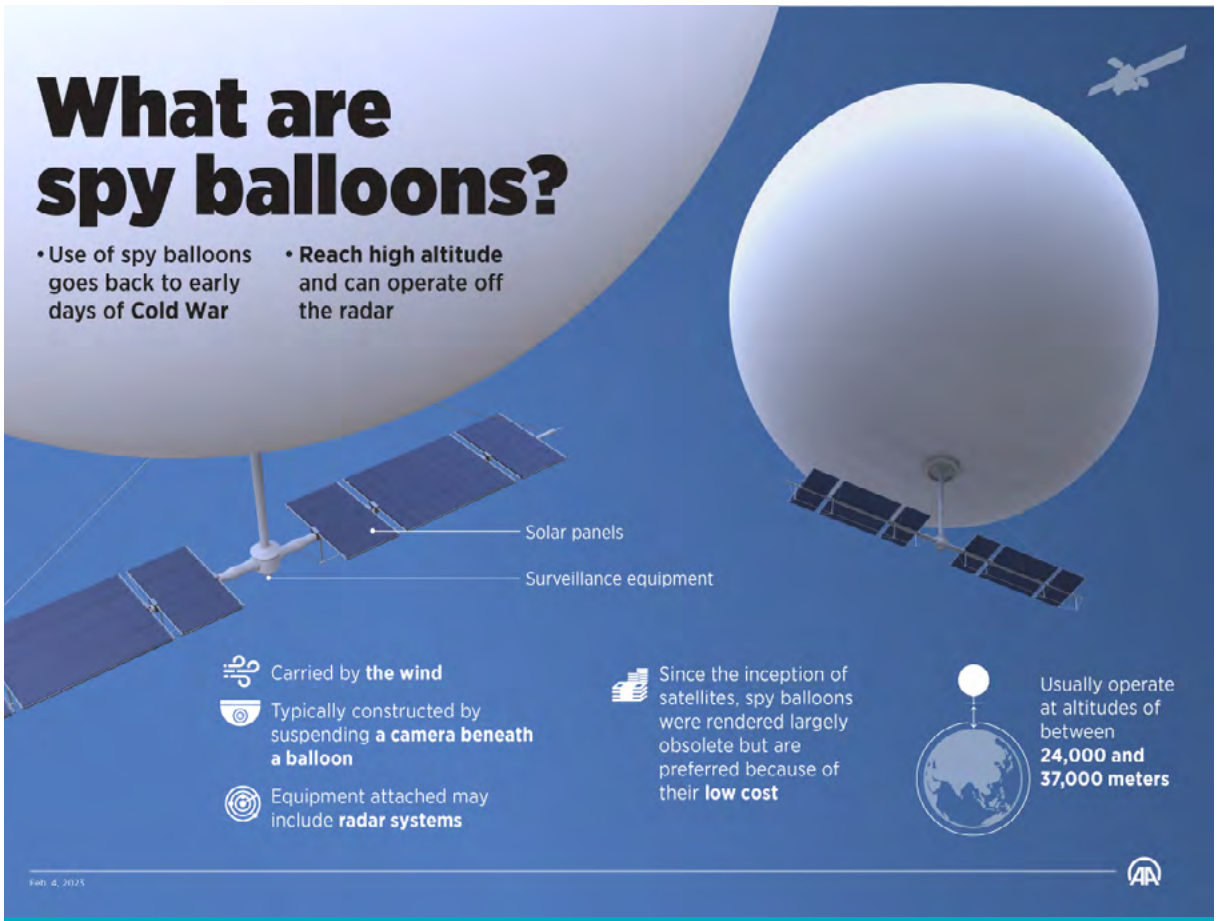


(Muhammed Selim Korkutata - Anadolu Agency)

Traditional Espionage

Besides the phenomenon of cyber espionage, China is also believed to be conducting covert operations to gather intelligence and gain access to sensitive information. This strategy consists of using agents or spies to infiltrate foreign governments or companies and monitoring target countries with some equipment.

In this context, the incident On February 4, 2023, was of particular significance. A suspicious balloon originating from China was detected in the United States airspace, the balloon was shot down by a US F-22 Raptor fighter jet after US President Joe Biden's stated: "We will take care of it" (Yilek, 2023).

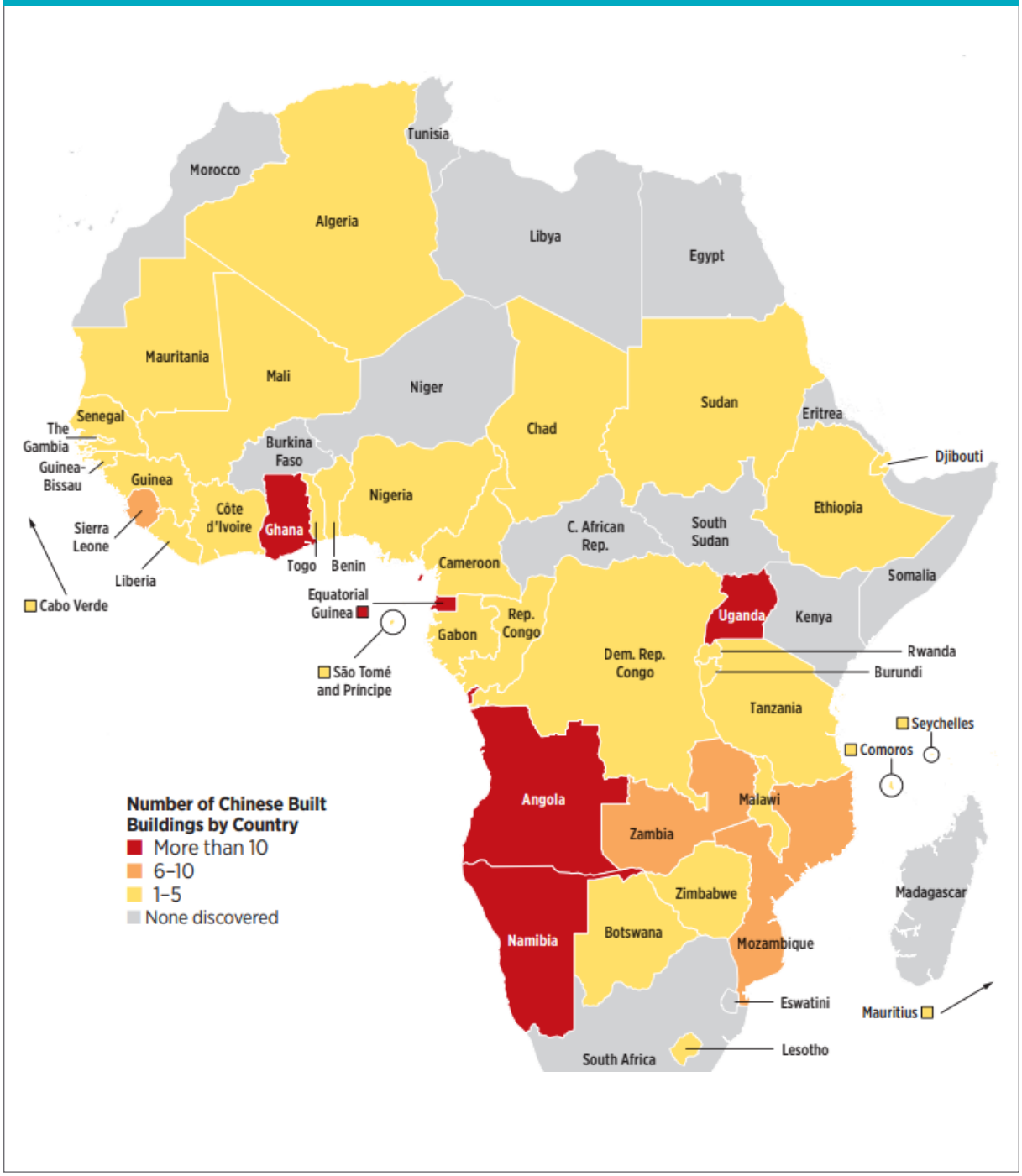


(Elmurod Usubaliev - Anadolu Agency)

Chinese intelligence-gathering activities internationally are also of concern. Beijing's involvement in Africa attracted the attention of the United States. It was claimed that China's military bases and different assets in these countries were used as intelligence, jeopardising the information security of US embassies in these countries.

The Chinese Communist Party (CCP) has undoubtedly gained considerable access in Africa after a frenzied two-decade-charm offensive. Chinese corporations have constructed at least 186 government buildings throughout Africa and at least 14 important intra-governmental telecommunication networks. It is noteworthy that all Chinese firms are required by law to assist the CCP in gathering information. Also, Beijing has given computers to at least 35 African nations' governments (Merservey, 2020).

Chinese-Constructed Government Buildings Across Africa



Moreover, China is the subject of allegations that it built an advanced and intense surveillance machine against its own citizens. Lookout, a cyber security firm based in the United States, claimed that China had placed spyware on phone applications to track the movements and conversations of Uyghurs inside and outside the country (Manson, 2022).

Amateurish Espionage or Scapegoating?

Alongside the highly mediatised episodes of the spy balloon and TikTok, China's conventional intelligence activities have been on the Western agenda for a long time. The FBI classifies Chinese intelligence gathering as the "greatest long-term threat to our nation's information" (Wray, 2020).

China's intelligence apparatus is governed by the National Intelligence Law of the People's Republic of China. It is the first national intelligence agency-related statute to be made public in China. Yet, none of the entities it applies to, such as the Ministry of State Security (MSS) and Ministry of Public Security, are officially mentioned in the law (MPS). The legislation states that "everyone is accountable for state security," which is consistent with China's overall system of state security law. Article 14 "requests the necessary support, assistance and cooperation from the relevant organs, organisations and citizens". According to Article 16, intelligence officers can "enter relevant prohibited areas and places; learn and inquire from relevant institutions, organisations and individuals; and read or collect related files, materials or items" (Saraswat, 2020). In this sense, the government imposes direct responsibility on its citizens.

Chinese intelligence collects information mostly through Chinese or Chinese-born students, medium and large-sized companies or academics and carries out an intelligence activity by combining this scattered information like puzzle pieces. Chinese intelligence has been accused of amateurism, as people who gather information for Chinese intelligence, but have not undergone professional intelligence training, are often exposed. In addition, China's use of people of Chinese origin in intelligence operations is often cited as a weakness (Mattis, 2010).

Peter Mattis (2010) argues that this perception of "amateurism" stems from the exposure of third parties providing intelligence for China. Stating that disclosing the information-gathering activities of Chinese companies abroad cannot be a basis for Chinese intelligence to be labelled as "amateur", Mattis (2010) states that those exposed are not Chinese intelligence officers but ordinary people who have not received intelligence training. Mattis also states that China does not only use people of Chinese origin to gather intelligence, and examples of this have recently emerged. According to Mattis (2010), staffing in the Chinese intelligence system is built on a three-stage system. While the first layer consists mainly of permanent intelligence officers, the second layer consists of contracted personnel who perform various tasks. Finally, the third layer, consisting of collaborators (companies, students, scientists, etc.), completes the manpower pyramid. Therefore, Chinese people living in Western countries are convenient for the latter type of activities (Mattis, 2010).

In this sense, China often comes to the fore in the context of human intelligence in espionage. For example, in September 2020, it was reported that the US cancelled the visas of 1,000 Chinese students and researchers. Authorities claimed the students had ties to the Chinese military and accused some of being spies (BBC, 2020).

Another issue in which China's intelligence capabilities were discussed was the use of the spy balloon. This technique was first used in the 18th century and is considered obsolete after the development of satellite technologies. While this technique is low-cost, it has another advantage over satellites: they can stay on a certain point longer than the orbital passage of the satellites. Also, satellites are more easily detected during their orbital transitions. It is also stated that such spy balloons do not attract attention because they can be considered as a civilian activity (Sables, 2023). Conversely, China's Foreign Ministry spokesperson Mao Ning accused the United States of "exaggerating the balloon issue for pure political manipulation" and said that her country rejected such an approach. The statement stated that the balloon was a Chinese civil aircraft used for meteorological research, and that it accidentally entered the US airspace after facing strong winds (Fujiyama, 2023).

While claims abound against China and the label of 'amateurism' sticks to its intelligence apparatus, China made spying allegations against the United States. As a result, China imposes restrictions on Western-owned social media platforms and 5G technology.

Subsequently, the Chinese authorities have banned access to Facebook, Google, Twitter, Instagram, Snapchat, Yahoo, Slack, and YouTube platforms. Beijing is determined to manage the internet within its borders, stating that these platforms violate the country's security (Shira, 2017). These accusations were validated by highly mediatised scandals, such as the Facebook-Cambridge Analytica affair, which breached the personally identifiable information of 50 million Facebook users in 2014 and sold them to politically motivated actors (Cadwalladr & Graham-Harrison, 2018).

Alongside cybersecurity measures, China also caught agents that it claims were working on behalf of the United States. The New York Times reported in October 2021, citing a leaked CIA cable, that the CIA has lost "a disturbing number of informants" recruited in recent years from countries, including China, admitting that the informants have been killed, captured, or compromised (Barnes & Goldman, 2021).

'Silent Watchers': US-China tension

With the G20 summit held in Indonesia on November 14, 2022, by Chinese President Xi Jinping and US President Joe Biden, diplomatic relations were established at the highest level between both countries (Bose & Widianto, 2022). However, after the spy balloon crisis, US Secretary of State Antony Blinken postponed his visit to China (Dag, 2023). Again, at the end of February, the US claimed that China is believed to be supplying arms to Russia. As a result, China was criticised by the international community (Horti & Landale, 2023). The assertive foreign policy approach under the Xi Jinping leadership, created an anti-Chinese front, and many countries came together in support of the US (Oguzlu, 2023).

Conversely, China is regularly inciting against US presence in the Indo-Pacific and South Pacific. Many analysts called the tension between the two countries a second "Cold War" and suggested that if it went on like this, the two countries might even experience an armed conflict towards the end of the current decade (Oguzlu, 2023). The military bases that China plans to establish in these regions drew the ire of Western governments, as well as the different military security agreements signed with different protagonists, such as the Solomon Islands and Cambodia (Gunia, 2022). The US is also concerned about Chinese access to advanced hi-tech and electronic technologies in Israel. China has emerged as one of the largest foreign investors in Israel's equivalent to Silicon Valley, sometimes called the Silicon Wadi.

In this context, it could be argued that the economic and military competition between the two countries fuels the recurrent allegations against China's espionage activities to limit Beijing's room for manoeuvre.



(XINHUA - Anadolu Agency)

Conclusion

China has emerged as one of the world's major powers. However, its relations with Western countries have witnessed recently more downs than ups, and China's growing influence has often been accompanied by accusations of spying on other countries.

Since 1998, China's Ministry of Defence has prepared white papers every year, informing its military attaches about the main issues facing Beijing. In the 2015 report, it was stated that the Chinese army switched from classical defence to active defence for the first time. Also, Chinese laws have raised concerns. Unlike democratic Western countries, China demands its citizens to work and cooperate with the state when necessary. It also mandated that internet companies cooperate with the Chinese government to reduce the anonymity of users. In this context, Western human rights organisations have issued multiple reports that Beijing keeps the minorities in its own country under tight surveillance and force its citizens abroad to engage in intelligence activities.

China stands out as a country that tries to shuffle the deck in the international chessboard. Against this background, Beijing resorts to intelligence gathering activities as is the case for other governments worldwide. However, China has been singled out because of its rising status in world affairs. In the ensuing battle for supremacy, the US intelligence community builds a narrative of present and imminent danger around Beijing's activities to create a wedge between China and other countries. After all, American elites have always felt the need to create an "other", a bogeyman to compete against.

References

Barnes, J. E., & Goldman, A. (2021, October 5). Captured, killed or compromised: C.I.A. admits to losing dozens of informants. The New York Times. Retrieved March 17, 2023, from https://www.nytimes.com/2021/10/05/us/politics/cia-informants-killed-captured.html

Berman, N., Maizland, L., & Chatzky, A. (2023, February 8). Is China's Huawei a threat to U.S. National Security? Council on Foreign Relations. Retrieved March 14, 2023, from https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security

BBC. (2020, September 10). US revokes visas for 1,000 Chinese students deemed security risk. BBC News. Retrieved March 18, 2023, from https://www.bbc.com/news/world-us-canada-54097437

Bose, N., & Widianto, S. (2022, November 15). Biden and XI clash over Taiwan in Bali but Cold War fears cool. Reuters. Retrieved March 18, 2023, from https://www.reuters.com/world/ahead-tense-g20-summit-biden-xi-meet-talks-2022-11-14/

Brown, C. S. (2022, December 12). The Huawei Ban explained: A complete timeline and everything you need to know. Android Authority. Retrieved March 17, 2023, from https://www.androidauthority.com/huawei-google-android-ban-988382/

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. Retrieved March 13, 2023, from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Clinch, M. (2018, August 17). China backs Turkey to overcome its economic crisis. CNBC. Retrieved March 12, 2023, from https://www.cnbc.com/2018/08/17/china-backs-turkey-to-overcome-its-economic-crisis.html

Dag, B. (2023, February 5). US shoots down Chinese 'spy' balloon. Anadolu Ajansı. Retrieved March 4, 2023, from https://www.aa.com.tr/en/asia-pacific/us-shoots-down-chinese-spy-balloon/2806384

Ellsworth, B. (2022, May 20). Canada bans Huawei from participating in country's 5G Wireless Networks. Anadolu Ajansı. Retrieved March 17, 2023, from https://www.aa.com.tr/en/americas/canada-bans-huawei-from-participating-in-country-s-5g-wireless-networks/2592818

Euronews. (2023, March 24). Which countries have banned TikTok and why? euronews. Retrieved March 24, 2023, from https://www.euronews.com/next/2023/03/23/which-countries-have-banned-tiktok-cybersecurity-data-privacy-espionage-fears

Fujiyama, E. W. (2023, February 6). China accuses us of indiscriminate use of force over balloon. AP NEWS. Retrieved March 14, 2023, from https://apnews.com/article/politics-united-states-government-china-north-america-f8b1c1bbf0fe7bcf8908c45e03c582c8

Gady, F.-S. (2015, May 27). China to embrace new 'active defense' strategy. – The Diplomat. Retrieved March 8, 2023, from https://thediplomat.com/2015/05/china-to-embrace-new-active-defense-strategy/

Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2014). World War C: Understanding nation-state motives behind today's advanced cyber attacks. FireEye, Milpitas, CA, USA, Tech. Rep., Sep.

Gehrke, J. (2020, September 23). Exclusive: Pompeo warns Turkey that Huawei threatens US military presence. Washington Examiner. Retrieved March 11, 2023, from https://www.washingtonexaminer.com/policy/defense-national-security/exclusive-pompeo-warns-turkey-that-huawei-threatens-us-military-presence

Habibi, N. (2022). The Belt and Road Initiative in the Eastern Mediterranean: China's Relations with Egypt, Turkey, and Israel. Middle East Briefs, 33970

Horti, S., & Landale, J. (2023, February 20). Ukraine War: Blinken says China might give weapons to Russia. BBC News. Retrieved March 19, 2023, from https://www.bbc.com/news/world-us-canada-64695042

Information Office of the State Council of the People's Republic of China, 2009. (2009, January). China's national defense in 2008 - programs.fas.org. programs.fas.org. Retrieved March 8, 2023, from https://programs.fas.org/ssp/nukes/2008DefenseWhitePaper_Jan2009.pdf

Information Office of the State Council The People's Republic of China. (2011, March). China's National Defense in 2010. Retrieved March 8, 2023, from https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/201104/t20110402_599668.html

Kanno-youngs, Z., & Sanger, D. E. (2021, July 19). U.S. ac-

cuses China of hacking Microsoft. The New York Times. Retrieved March 9, 2023, from https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html

Lewis, J. A., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage.

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (Eds.). (2015). China and cybersecurity: Espionage, strategy, and politics in the digital domain. Oxford University Press, USA.

Mandiant, M. (2013, September). APT1: Exposing one of China's cyber espionage units. Mandiant. Retrieved March 6, 2023, from https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units

Manson, K. (2022, November 10). Lookout researchers say spyware tied to China is targeting apps used by Uyghurs. Bloomberg.com. Retrieved March 18, 2023, from https://www.bloomberg.com/news/articles/2022-11-10/lookout-researchers-say-spyware-tied-to-china-is-targeting-apps-used-by-uyghurs

Mattis, P. (2010). Shriver Case Highlights Traditional Chinese Espionage. Jamestown Foundation China Brief, 10.

Meservey, J. (2020). Government Buildings in Africa Are a Likely Vector for Chinese Spying. Heritage Foundation.

News, V. O. A. (2020, April 30). China, caught meddling in past two US elections, claims 'not interested' in 2020 vote. VOA. Retrieved March 12, 2023, from https://www.voanews.com/a/east-asia-pacific_china-caught-meddling-past-two-us-elections-claims-not-interested-2020-vote/6188474.html

Ni, V. (2021, December 15). Documents link Huawei to Uyghur surveillance projects, report claims. The Guardian. Retrieved March 17, 2023, from https://www.theguardian.com/technology/2021/dec/15/documents-link-huawei-uyghur-surveillance-projects-report-claims

Oguzlu, T. (2023, February 8). 3 soruda - blinken'ın iptal Edilen çin gezisi: Abd-çin Ilişkileri Nereye Gidiyor? Anadolu Ajansı. Retrieved March 15, 2023, from https://www.aa.com.tr/tr/analiz/3-soruda-blinken-in-iptal-edilen-cin-gezisi-abd-cin-iliskileri-nereye-gidiyor/2811186

Paul, K., & Bhuiyan, J. (2023, March 23). TikTok CEO grilled for over five hours on China, drugs and Teen Mental Health. The Guardian. Retrieved March 24, 2023, from https://www.theguardian.com/technology/2023/mar/23/tiktok-shou-zi-chew-congress

Saraswat, A. (2020, September 5). Understanding the national intelligence law of china: Why India banned Tik Tok? Diplomatist. Retrieved March 18, 2023, from https://diplomatist.com/2020/09/05/understanding-the-national-intelligence-law-of-china-why-india-banned-tik-tok/

Sganga, N. (2022, October 26). China-linked influence campaign targeting U.S. midterms, security firm says. CBS News. Retrieved March 7, 2023, from https://www.cbsnews.com/news/dragonbridge-china-us-midterm-elections-influence-campaign-mandiant/

TRT Haber. (2023, March 22). Abd Kongresindeki Kritik Ifade öncesi "Tiktok" tartışması alevlendi. Son Dakika Haberler. Retrieved March 23, 2023, from https://www.trthaber.com/haber/dunya/abd-kongresindeki-kritik-ifade-oncesi-tiktok-tartismasi-alevlendi-754917.html

Viswanatha, A., Lubold, G., & O'Keeffe, K. (2023, March 6). WSJ News exclusive | Pentagon sees giant cargo cranes as possible Chinese spying tools. The Wall Street Journal. Retrieved March 9, 2023, from https://www.wsj.com/articles/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade

Weissbrodt, D. (2013). Cyber-conflict, cyber-crime, and cyber-espionage. Minn. J. Int'l L., 22, 347.

Yilek, C. (2023, February 20). What we know so far about the Chinese spy balloon and the other objects the U.S. shot down. CBS News. Retrieved March 17, 2023, from https://www.cbsnews.com/live-updates/chinas-spy-balloon-unidentified-objects-shot-down-what-we-know-so-far/

TRT WORLD
research centre

TRTWORLD
research
centre