AMERICAN FOREIGN POLICY COUNCIL


# China Policy Monitor No. 1589

April 1, 2024 **Joshua Eisenman**

**Related Categories:** Cybersecurity and Cyberwarfare; Democracy and Governance; Intelligence and Counterintelligence; Public Diplomacy and Information Operations; China; New Zealand; United Kingdom ; United States

**XI: CHINA'S OFFICIALS UNPREPARED FOR "GREAT STRUGGLE"**
"After decades of peaceful rule, many party members and cadres have not experienced the test of life and death, lacking the tempering of brutal struggles and harsh environments. They love to seek comfort and enjoyment, rest on their laurels and become complacent. They will panic and lose their confidence easily amid the great struggle with many new historical characteristics," Xi Jinping told the 2nd plenum of the 20th Central Commission for Discipline Inspection (CCDI) in January 2023. The speech, published this week in *Qiushi*, preceded the CCDI's campaign against "lying flat," or doing the bare minimum. Tasked with maintaining social stability in tough economic times, China's officials are facing pay cuts, heavy workloads, never-ending inspections, and political study sessions. Low morale and the fear of being punished if they take bold initiatives that fail have prompted many to err on the side of restraint. The CCDI should be strict, but "not control people until they can't do anything, making officials hesitant and fearful to act, and turn the government into a gloomy pool of stagnant water," Xi said. (*South China Morning Post*, March 16, 2024)

**SEVEN CHINESE HACKERS INDICTED FOR TARGETING U.S. OFFICIALS, COMPANIES**
A U.S. federal court in New York has indicted seven PRC hackers for their part in a years-long effort to collect data from millions of Americans. Posing as prominent American journalists, the hackers sent thousands of malicious emails to senior U.S. officials in the White House and Justice Department, as well as other federal agencies and both Democratic and Republican senators in more than ten states. They also targeted "some of America's most vital critical infrastructure sectors," including U.S. defense contractors, said the U.S. Treasury Department. Working for China's Ministry of State Security, the seven men used the Wuhan Xiaoruizhi Science and Technology Company as a cover for their illicit activities. The State Department is offering a $10 million reward for information on the seven men. (*CNN*, March 25, 2024)

**CHINA'S CYBERATTACKS ON UK, NZ PARLIAMENTARIANS**
Britain has accused China of conducting "a large-scale espionage campaign," including malicious cyberattacks against its democratic institutions and members of Parliament. Between 2021 and 2022, the PRC-affiliated cyber hacking group dubbed Advanced Persistent Threat 31 (APT31) targeted the email accounts of MPs and it was "highly likely" that they also hacked into and stole information from the UK Electoral Commission, the UK National Cyber Security Centre (NCSC) found. These activities are "indicative of a wider pattern of unacceptable behavior" from Beijing, said NCSC Director of Operations Paul Chichester. In response, London has summoned China's ambassador, sanctioned a front company and at least two members of APT31. Meanwhile, this week New Zealand also accused China of carrying out cyberattacks against its Parliament back in 2021. (*New Zealand Herald*, March 25, 2024; *Next Web*, March 26, 2024)

**FIVE CHINESE AND 1 PAKISTANI KILLED IN SUICIDE BOMBING**
Five Chinese nationals and their Pakistani driver have been killed in a suicide bombing attack in Pakistan. The Chinese engineers were heading from Islamabad to a dam construction site in Dasu, Khyber Pakhtunkhwa province when their convoy was hit. The Dasu Hydropower Project, built with China's assistance, has been targeted before; in 2021, nine Chinese were killed in a bus bombing. The most recent bombing is the third major attack on Chinese interests in a week, and follows assaults on an airbase and a port in Baluchistan. Pakistan's Foreign Minister, Ishaq Dar, condemned the attacks, which come as Prime Minister Shehbaz Sharif is preparing to visit Beijing. (*Newsweek*, March 26, 2024)

**FOREIGN CONSULTING FIRMS A "COVER" TO STEAL STATE SECRETS, MINISTRY SAYS**
China's Ministry of State Security said in a post on its official WeChat account that foreign spy agencies are using consulting as "cover" to steal classified information from the PRC, posing "major risks to national security." The post includes a video in which an overseas consultancy conducted a review of a Chinese company with the stated purpose of assisting its overseas listing but used the process to gain access to core data and state secrets on behalf of foreign intelligence agencies. Illegally obtaining commercial secrets for "the containment and suppression of China's advantageous industries" amounts to acting as "an accomplice" in espionage, infiltration and instigation, the ministry warned. (*South China Morning Post*, March 28, 2024)

[EDITOR'S NOTE: The country's revised counter-espionage law, which came into effect in July of 2023, expands both the definition of spying and the powers of national security agencies to investigate it. The newly amended state secrets law, which comes into effect in May, adds a dozen new clauses that expand the depth and reach of its coverage.]

---