AMERICAN FOREIGN POLICY COUNCIL

China Reform Monitor No. 1463

May 12, 2021 **Joshua Eisenman**

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Human Rights and Humanitarian Issues; International Economics and Trade; China; Europe; Japan; Southeast Asia; Taiwan

CHINA IS FUELING AMERICA'S QANON CONSPIRACY THEORIES
China is spreading QAnon conspiracy theories online, fueling a movement that has become a domestic terrorism threat in the U.S. For most of last year, Russians dominated foreign QAnon posts, but they have been overtaken by those from China. Nearly one-fifth of 166,820 QAnon-related Facebook posts between January 2020 and the end of February 2021 originated from overseas, and of that number 58 percent came from China – more than double those from Russia. "We have enough problems without the amplification of conspiracy theories by foreign actors, and that foreign impact really does stir up a hornet's nest. In China, nothing is going to be done without the Chinese government being aware of it. I think there is at a minimum tacit support for the amplification," noted Jason Blazakis of the Soufan Center, a top counterterrorism research center. (Yahoo! News, April 19 2021)

CHINA'S PRESSURE ON CANADA NOT TO HONOR TAIWAN'S TSAI BACKFIRES
Back in November, Canada's Halifax Forum, an annual conference of officials and experts, was set to give its John McCain Prize for Leadership in Public Service to Taiwan's President, Tsai Ing-wen. However, those plans were scrapped after Defense Minister Harjit Sajjan threatened to pull out of the forum and cut its funding. The ultimatum was delivered by Deputy Defense Minister Jody Thomas on a call with Halifax Forum President Peter Van Praagh. Thomas cited negotiations between Ottawa and Beijing over the "two Mikes" as a reason for not upsetting Beijing. The think tank, however, has held firm on its plans. "We were always going to give this award to President Tsai. We are giving it to Tsai. We are not wavering from that," said one Halifax official. Canada's House of Commons has also weighed in, passing a resolution calling President Tsai the ideal candidate for the prize and demanding the government continue funding the Forum after it honors Tsai at a different event this Spring. (*Washington Post*, April 15, 2021)

[EDITOR'S NOTE: China has been holding Canadian citizens Michael Kovrig and Michael Spavor in detention for more than two years, and is trying to trade them for Huawei chief financial officer Meng Wanzhou, who is under house arrest in Vancouver as she fights extradition to the U.S.]

HUAWEI HAD ACCESS TO CALLS MADE BY 6.5 MILLION DUTCH
Huawei could have monitored all calls made by the 6.5 million users of KPN, one of the Netherlands' largest mobile phone networks, without its knowledge. KPN started using Huawei technology in 2009 and was soon warned about the problem by Dutch intelligence services. Still, KPN awarded contracts for its 3G and 4G networks to Huawei, claiming it had "never observed that Huawei took client information." In 2019, a Dutch government task force called for stronger vetting of telecoms equipment suppliers. Last year, KPN became one of the first European operators to exclude Huawei from its 5G network, and Amsterdam announced tighter restrictions for equipment suppliers, including background checks for staff. (*Guardian*, April 19, 2021)

TOKYO: PLA "HIGHLY LIKELY" BEHIND SCORES OF CYBERATTACKS
Japan's police are investigating cyberattacks on about 200 companies and research organizations, including the Japan Aerospace Exploration Agency (JAXA), by a hacking group linked to the Beijing. Police believe the hacks were conducted in 2016-17 by "Tick," and that "the involvement of China's PLA is highly likely," according to Chief Cabinet Secretary Katsunobu Kato. A suspect in the JAXA case, a Chinese systems engineer, gained access to a rental server by registering himself under a false identity to launch the cyberattacks. Cyberattacks were among the rising security threats from China that President Joe Biden and Japanese Prime Minister Yoshihide Suga discussed at the White House on April 16th. (Associated Press, April 20, 2021)

PLA HACKERS TARGET SOUTHEAST ASIAN GOVERNMENTS AND MILITARIES
Since at least June 2019, a PLA hacking group known as the Naikon group has been accessing military and government institutions throughout Southeast Asia to steal their secrets and data. Naikon conducts espionage against Asian countries, and is focused primarily on military, economic, diplomatic and government targets in Australia, Indonesia, the Philippines and Vietnam. The group uses software vulnerabilities in Outlook Item Finder, McAfee's VirusScan On-Demand Scan Task Properties, etc. to mask its malicious hacking techniques. The hackers used a backdoor to move around in compromised systems, retain access to them and upload files to Dropbox. (Cyberscoop, April 29, 2021)