AMERICAN FOREIGN POLICY COUNCIL

China Reform Monitor No. 1365

March 26, 2019 **Joshua Eisenman**

Related Categories: Democracy and Governance; Human Rights and Humanitarian Issues; International Economics and Trade; Military Innovation; Science and Technology; China; Europe

CHINESE HACKERS TARGET U.S. UNIVERSITIES FOR MILITARY TECH
Since at least April 2017, China's state-backed hackers have been stealing military maritime technology from more than 27 universities in the U.S., Canada and Southeast Asia, including the University of Hawaii, the University of Washington, MIT, Duke and Penn State. The universities' networks were connecting regularly with servers in China linked to a well-known hacking group. Most of the universities targeted have research centers on undersea technology, faculty with relevant experience, and are linked to an unnamed Massachusetts oceanographic institute. The same perpetrators have also stolen submarine missile plans and ship-maintenance data from U.S. Navy contractors. China's hackers favor universities because they have weaker defenses compared to the U.S. military and its contractors. (*Wall Street Journal*, March 6, 2019)

HUAWEI'S PRESENCE HURTS U.S.-HUNGARY TIES
U.S. Secretary of State Mike Pompeo has warned Hungarian Foreign Minister Peter Szijjarto about "the dangers of allowing China to gain a bridgehead in Hungary" – a reference to the growing presence exhibited by China's state-connected telecom giant Huawei in the European nation. Pompeo said: "If that equipment is co-located in places where we have important American systems, it makes it more difficult for us to partner alongside them. We want to make sure we identify [to] them the opportunities and the risks associated with using that equipment."

Beijing has claimed that Washington's concerns about Huawei are inauthentic, and are designed to help American companies gain an advantage over foreign competitors. "That sounds like a lot of mirror imaging to me," counters U.S. Assistant Secretary of State for International Security and Nonproliferation Christopher Ford. "[China] has actually been extraordinarily grand in its ambitions to do just that sort of thing with Chinese companies. Cyber-facilitated theft of intellectual property, for example, has become notorious around the world...in order to advantage its own national champion industries in particular sectors." (Voice of America, February 11, 2019)

MASSIVE DATABASE LEAKS OFFER A GLIMPSE INTO XINJIANG
A security researcher has found and disclosed two open databases live-tracking the locations of residents and vehicles in Xinjiang. The first database includes national ID numbers, ethnicity, nationality, phone number, date of birth, home address, employer, and photos for about 2.6 million people. Over 24 hours, 6.7 million individual GPS coordinates were stored in the database, linking individuals to various public camera streams and identification checkpoints with location tags such as "hotel," "mosque," and "police station." The database is owned by SenseNets, a private AI company advertising facial recognition and crowd analysis technologies. The second open database tracks the movements of millions of cars and pedestrians and connects security cameras with WeChat profiles in order to link each person's image with their identity. (ZDNet, February 14, 2019; Electronic Frontier Foundation, March 1, 2019)

CHINA AND RUSSIA EXPAND COOPERATION IN CIVILIAN MONITORING
China and Russia are cooperating in the design and production of "civilian navigation equipment...including standards of control and management of traffic across the Russian-Chinese border." Russian President Vladimir Putin has issued an executive order ratifying the agreement on cooperation between the GLONASS and BeiDou navigation satellite systems. Signed in Beijing at a November 2018 prime ministerial, it lays the "organizational and legal fundamentals for the joint use of the Glonass and BeiDou global navigation satellite systems and their functionalities, the development of navigation technologies based on the Glonass and BeiDou systems, and the exchange of practices of civilian navigation satellite services." Networks stations from both systems will be deployed in both countries so they can operate on each other's territories. (Interfax, March 1, 2019)

CHINA BANS 23 MILLION FROM TRAVELING

China has blocked 23 million travelers from purchasing train or plane tickets due to bad social credit scores. By the end of 2018, travelers had been banned from buying 17.5 million flights and 5.5 million train tickets. Approximately 3.5 million people or companies have paid taxes or debts under the credit system, and large numbers have been prevented from buying insurance, real estate or investment products. Journalist Liu Hu, for example, was placed on a list of "dishonest persons" who is "not qualified" to buy a plane ticket, buy property or take out a loan. "There was no file, no police warrant, no official advance notification. They just cut me off from the things I was once entitled to," said Liu. "What's really scary is there's nothing you can do about it. You can report to no one. You are stuck in the middle of nowhere." (*London Globe and Mail*, January 3, 2019; *Wired*, January 21, 2019; Fox News, March 3, 2019)
