AMERICAN FOREIGN POLICY COUNCIL

China Reform Monitor No. 1431

September 1, 2020 **Joshua Eisenman**

Related Categories: Cybersecurity and Cyberwarfare; Democracy and Governance; Human Rights and Humanitarian Issues; International Economics and Trade; Corruption; Latin America; Middle East; Taiwan

CHINA'S HACKERS PILLAGE TAIWAN'S SEMICONDUCTOR INDUSTRY
Between 2018-19, China-based hackers attacked seven of Taiwan's top semiconductor manufacturers, scouring their internal networks for intellectual property to steal. The series of intrusions—called Operation Skeleton Key because the attackers used a method known as the "skeleton key injector" technique—targeted the companies' source code, software development kits, and chip designs. The hackers exploited the firms' VPN software to break into their corporate networks, then altered the software authentication program, and planted malicious code that allowed them to access others on those networks. (*Wired*, August 6, 2020)

CHINA'S HACKERS STEAL DATA FROM TEN TAIWANESE AGENCIES
Since 2018, four mainland China-based hacking groups – Blacktech, Taidoor, MustangPanda, and APT40 – have attacked at least ten Taiwanese central and local-level government agencies and gained access to the email accounts of 6,000 officials in order to steal important documents and data. Government agencies contracted Taiwanese providers to help them upgrade and maintain their data systems, but the local firms then subcontracted with Chinese hackers offering free remote access and VPNs to carry out remote maintenance of the government data systems. "Through these contractors, the hackers set up relay stations which they used to attack government departments to obtain the important files or information they wanted," said Liu Chia-zung, deputy director of the bureau's Cyber Security Investigation Office. Once inside, the hackers planted a back door allowing them to access the email accounts of at least 6,000 officials. Afterward, the hackers removed all traces, making it difficult to identify what information they stolen. The attacks "pose a serious threat to government operations and cybersecurity," Taiwan's Investigation Bureau has said. (*South China Morning Post*, August 19, 2020)

TAIPEI ANNOUNCES BAN ON CHINA'S STREAMING SERVICES
Taiwan's National Communications Commission has announced new rules prohibiting its citizens and companies from distributing Chinese streaming services such as Tencent Video and iQiyi, which are akin to Netflix. They stream licensed content, and also produce original television shows and movies that have become popular with Mandarin-speaking audiences. Until now, these services have been "illegally" partnering with local broadcasters and distributors that provide their video content in Taiwan. The move effectively bans these and other Chinese tech giants from operating streaming video services on the island. Tencent's video service has 114 million subscribers and iQiyi has 105 million, mostly in mainland China. (CNN, August 19, 2020)

SCORES OF CHINESE FISHING VESSELS NEAR GALAPAGOS ISLANDS – ECUADOR
Around 150 of the more than 300 mostly Chinese fishing vessels operating near the Galapagos Islands have turned off their satellite tracking systems to prevent Ecuador's navy from monitoring them. Some of the ships, which continue to illegally fish the waters of the ecologically protected region, have also changed their names. "It is a breach (of protocol) on the high seas, because they do not want us to know what they are doing and the activities they carry out," Ecuadorian Defense Minister Oswaldo Jarrin has said. Ecuador wants to prevent illegal fishing off its coast, but must also avoid angering China – its largest financier and a major market for its shrimp exports. Despite China's promised "zero tolerance" policy toward illegal fishing, each summer since 2017 the Chinese fishing fleet has arrived to hunt rare marine species like the giant squid and hammerhead shark. (Reuters, August 18, 2020)

SAUDI ARAMCO SUSPENDS $10 BILLION REFINERY JOINT VENTURE WITH CHINA
Citing an "uncertain market outlook," Saudi Arabia's state oil company, Saudi Arabian Oil Co., i.e., Aramco, has suspended a $10 billion deal to build a 300,000-barrel-a-day refining and petrochemicals complex in Liaoning, China. The project's three partners – Aramco, China North Industries Group Corp., i.e., Norinco, and China's Panjin Sincen Industrial Group Co. Ltd – all declined to comment on the status of the joint venture, Huajin Aramco Petrochemical Co., which Crown Prince Mohammed bin Salman touted as a landmark bilateral deal when he visited Beijing in February 2019. Riyadh was to supply as much as 70% of the crude for the refinery that Chinese firms will now complete on their own. (Bloomberg, August 21, 2020)