OPINION: THIS CYBERSECURITY AWARENESS MONTH, SPY CHIEFS WARN OF CHINA'S EXPANDED EFFORT TO STEAL TECHNOLOGIES - INSIDE SOURCES

Posted on October 30, 2023 by Doug Kelly | Inside Sources

An unprecedented summit of intelligence chiefs from five nations warned that China's espionage efforts are increasingly focused on Silicon Valley tech companies rather than the U.S. government.

The recent gathering was the first-ever public meeting of the so-called "Five Eyes" intelligence-sharing network, consisting of the heads of the Federal Bureau of Investigation (FBI), Britain's MI5, and the intel leaders from Australia, Canada, and New Zealand. Held at Stanford University in the heart of the U.S. tech industry, and during National Cybersecurity Awareness Month, the group met to map out strategies to prevent China from stealing even more Western trade and innovation secrets.

FBI Director Christopher Wray was blunt in his assessment, noting, "There is no greater threat to innovation than the Chinese government" and that "the Chinese government is absolutely the biggest threat we face."

The spy chiefs' warning to business leaders in democratic countries was stark and clear: China is hyper-focused on stealing emerging technologies in AI, quantum technology, robotics, biotechnology, and automation, which could transform China both economically and from a security standpoint. Alarmingly, China is already using AI to elevate the sophistication of its hacking efforts.

To grasp the magnitude of China's espionage machinery, consider that:

- China's hacking program is bigger than every major nation combined and is growing. In fact, the FBI has seen a 1,300 percent increase in investigations linked to the Chinese government's theft of secrets.
- China has stolen more personal and corporate data than every nation combined. All told, China steals an estimated $500 billion annually of U.S. intellectual property.
- China's cyber personnel dwarf the FBI's cyber teams, outnumbering them by 50 to one. Its covert, state-backed Cyber Corps unit

boasts 100,000 members, from hackers to linguists, all dedicated to conducting multi-year campaigns against critical U.S. entities.

- Britain's MI5 head divulged that Beijing solicited 20,000 Britons for trade secrets. He said an estimated 10,000 British businesses were at risk from China.

Beyond hacking, China deploys other tactics, such as embedding sleeper agents in Western companies and mandating technology transfers through joint ventures. Beijing has also enacted laws forcing any person of Chinese origin globally to aid its intelligence services, essentially demanding "hand over secrets, or face consequences."

Yet, in the face of these revelations about China's designs on American technology, some Western lawmakers seem to be inadvertently playing into Beijing's hands. They are targeting America's leading tech innovators with excessive new regulations that could hand China a competitive advantage in the global tech race. For example, the European Union (EU) recently designated six companies as "gatekeepers" under its Digital Markets Act (DMA). Alarmingly, five of the six gatekeepers — Alphabet, Amazon, Apple, Meta, and Microsoft — are U.S.-based, and 21 of the 22 platform services requiring compliance are owned by American companies. The DMA's restrictions apply to no EU firms and only one Chinese company.

Domestically, too, some U.S. policymakers and agencies are pushing for stringent new regulations on our tech leaders, including new antitrust rules, tough restrictions on mergers and acquisitions, and attempts to create a U.S.-iteration of the DMA.

Each of these actions is short-sighted, risky, and threatens to stifle the very innovation that is pivotal for our national security and economic prosperity. Policymakers must recognize the looming threat from China and accelerate innovation rather than hamstring it. It matters greatly which country – and which set of values – builds the future.