ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

November 25, 2020

THE ELEMENTS OF THE CHINA CHALLENGE

The Policy Planning Staff, Office of the Secretary of State | November 2020

Awareness has been growing in the United States — and in nations around the world — that the Chinese Communist Party (CCP) has triggered a new era of great-power competition. Yet few discern the pattern in China's inroads within every region of the world, much less the specific form of dominance to which the party aspires. The CCP aims not merely at preeminence within the established world order — an order that is grounded in free and sovereign nation-states, flows from the universal principles on which America was founded, and advances U.S. national interests —but to fundamentally revise world order, placing the People's Republic of China (PRC) at the center and serving Beijing's authoritarian goals and hegemonic ambitions. In the face of the China challenge, the United States must secure freedom. China is a challenge because of its conduct. Modeled on 20th-century Marxist-Leninist dictatorship, the CCP eventually spurred rapid modernization and produced prodigious economic growth — thanks in no small measure to the party's decision in the late 1970s to embrace free-market elements and to the decision by the United States and nations around the world to engage, and welcome commerce with, China. The party today wields its economic power to co-opt and coerce countries around the world; make the societies and politics of foreign nations more accommodating to CCP specifications; and reshape international organizations in line with China's brand of socialism. At the same time, the CCP is developing a world class military to rival and eventually surpass the U.S. military.

Read the full article here.

JUSTICE DEPT.'S CHINA FOCUS LIKELY TO CONTINUE UNDER BIDEN

Eric Tucker | Star Tribune | November 19, 2020

President Donald Trump has identified China as the country's biggest foe and the Justice Department mirrored that emphasis over the last four years with a drumbeat of cases against defendants ranging from hackers accused of targeting intellectual property to professors charged with grant fraud. But even after Democrat Joe Biden's administration arrives, the law enforcement focus on China may not look radically different, in part because of actions by Beijing that U.S. officials, lawyers and analysts say run afoul of international norms. Even if the anti-China rhetoric is cooled in the White House, cases against agents of the Chinese government may well continue apace, especially since some of the focus — including against trade-secret theft — preceded the Trump administration. "I think this is going to continue because it's not really up to the U.S. It's the Chinese who are being really aggressive," said James Lewis, a senior vice president at the Center for Strategic and International Studies.

Read the full article here.

CHINA'S 5G CHALLENGE TO THE U.S. IS FOR … THE FUTURE

Shay Stautz | Foreign Policy Research Institute | November 24, 2020

5G is the latest generation of wireless communications technology (we've had about one every decade since the 1980s), and it means the future as we have envisioned it in movies—driverless cars, autonomous combat craft, drone deliveries, ubiquitous robotic manufacturing, smart homes, and advanced precision medicine; the list goes on and on. It basically is the infrastructure that everything requiring very high data communications flows through—more than 100 times faster than "4G" communications, and it requires the deployment of new technology and infrastructure to use. The next-generation network will transmit data over higher frequency signals, or waves, that are closer together, travel shorter distances, and are easily obstructed. This means more and smaller antennas about the size of a pizza box (some estimate as many as 3-10 times the number of existing transmitting sites) will be needed to cover the same area as 4G networks. This new communications infrastructure will provide the backbone of what Klaus Schwab referred to the "Fourth Industrial Revolution," spawning new types of companies built on "digital platforms," such as trailblazers like Uber and Netflix.

Read the full article here.

HOOVER INSTITUTION: CHINA'S GLOBAL SHARP POWER

Hoover Institution Weekly Alert | November 22, 2020

This weekly newsletter collects articles, reports and other media from across the world to illustrate the actions and behaviors of the Chinese Communist Party (CCP). The newsletter arose from the need to provide transparency to the citizens of liberal democracies of the scope and scale of China's sharp power initiatives and the harms those activities cause to the Chinese people and the rest of the world. As Xi Jinping stressed to the Party's leadership in late 2017, "Government, the military, society and schools, north, south, east and west – the party leads them all." This newsletter takes the Party's role seriously and examines the impact on the world of the Party's policies as they tighten their one-party rule.

Read the full article here.

WHICH COUNTRIES AND HACKERS ARE TARGETING COVID VACCINE DEVELOPERS?

Dan Sabbagh | The Guardian | November 22, 2020

Russia's best-known hacker groups – Fancy Bear and Cozy Bear – are considered to be linked to the country's intelligence organisations, according to western security agencies. Fancy Bear, the better known of the two, is linked to GRU military intelligence and is accused of being behind the hack of US Democratic party computers in the run-up to the 2016 presidential election, the product of which was widely leaked. Microsoft, which calls the group Strontium, last week accused Fancy Bear of targeting Covid-19 vaccine makers by using "password spray and brute force login attempts" – attacks that use "thousands or millions" of rapid attempts to obtain network access by guessing the password. Cozy Bear, linked variously to Russia's domestic FSB and foreign SVR agencies, was accused by Britain's NCSC agency of targeting drug research labs in the UK, the US and Canada in July. Its goal, NCSC said, was likely to be "stealing information and intellectual property relating to the development and testing of Covid-19 vaccines".

Read the full article here.

WHAT AN AUSTRALIAN-STYLE PUSH AGAINST CHINESE INTERFERENCE MIGHT LOOK LIKE

Evan Dyer | CBC | November 24, 2020

Some Australians see the country's new powers to stop foreign interference as an overdue shift from complacency to vigilance, while others have warned of the dangers of a McCarthyite moral panic. But all can agree that Australia's approach to foreign meddling in its politics, universities and public debate has changed a great deal in recent years. Last week, the Canadian House of Commons voted 179-146 for this country to adopt a plan similar to Australia's to counter meddling by the People's Republic of China. Experts in Canada and Australia suggest that such a change would set Canada on a much more aggressive path in countering China's inroads into this country's institutions. Conservative foreign affairs critic Michael Chong's motion requires the government to "develop a robust plan, as Australia has done, to combat China's growing foreign operations here in Canada and its increasing intimidation of Canadians living in Canada, and table it within 30 days of the adoption of this motion."

Read the full article here.

HACKERS 'TRY TO STEAL COVID VACCINE SECRETS IN INTELLECTUAL PROPERTY WAR'

Dan Sabbagh | The Guardian | November 22, 2020

State-sponsored hackers from China, Russia, Iran and North Korea are engaged in concerted attempts to steal coronavirus vaccine secrets in what security experts describe as "an intellectual property war". They accuse hostile-state hackers of trying to obtain trial results early and seize sensitive information about mass production of drugs, at a time when a range of vaccines are close to being approved for the public. Previously the hackers' primary intention was to steal the secrets behind the design of a vaccine, with hundreds of drug companies, research labs and health organisations from around the world targeted at any one time. The cyber struggle involves western intelligence agencies, including Britain's National Cyber Security Centre, who say they are committed to protecting "our most critical assets". But they discuss only a fraction of their work in public. Instead they work behind the scenes with drug companies, research labs and cybersecurity specialists, who are more easily able to describe the everyday hacking attempts in what amounts to a worldwide battle.

Read the full article here.

DOES U.K.'S HUAWEI BAN GO FAR ENOUGH IN ACTUALLY BANNING THE COMPANY?

Basit Mahmood | Newsweek | November 24, 2020

Telecoms giants in the U.K. could face fines of up to £100,000 ($133,000) a day, should they fail to meet targets for higher security requirements which are aimed at phasing out Huawei equipment from the country's 5G network. The measures are part of a new Telecommunications Security Bill which aims to ban the involvement of Chinese firm Huawei. The bill is the first to enshrine the banning of the Chinese company's involvement in the UK's 5G network into law. The government says that the bill will boost the security standards of the UK's telecoms networks and remove the threat of high-risk vendors. In July, after pressure from the Trump administration, the U.K. decided to ban the use of Huawei in 5G networks from the end of 2027 because of concerns that U.S. sanctions on chip technology meant the Chinese company would not be a reliable supplier and could also be used to carry out espionage on behalf of the Chinese state. The U.K. government also banned mobile providers from buying new Huawei 5G equipment after December 31.

Read the full article here.

EXCLUSIVE: IN LATEST CHINA JAB, U.S. DRAFTS LIST OF 89 FIRMS WITH MILITARY TIES

Karen Freifeld | Reuters | November 22, 2020

The Trump administration is close to declaring that 89 Chinese aerospace and other companies have military ties, restricting them from buying a range of U.S. goods and technology, according to a draft copy of the list seen by Reuters. The list, if published, could further escalate trade tensions with Beijing and hurt U.S. companies that sell civil aviation parts and components to China, among other industries. A spokesman for the U.S. Department of Commerce, which produced the list, declined to comment. Speaking in Beijing, Chinese Foreign Ministry spokesman Zhao Lijian said China "firmly opposes the unprovoked suppression of Chinese companies by the United States." What the United States is doing severely violates the principle of market competition and international norms for trade and investment that the U.S. claims to uphold, he added. Chinese companies have always operated in accordance with the law and strictly follow local laws and regulations when operating overseas, including in the United States, Zhao said. Commercial Aircraft Corp of China Ltd (COMAC), which is spearheading Chinese efforts to compete with Boeing and Airbus, is on the list, as is Aviation Industry Corporation of China (AVIC) and 10 of its related entities. The list is included in a draft rule that identifies Chinese and Russian companies the U.S. considers "military end users," a designation that means U.S. suppliers must seek licenses to sell a broad swath of commercially available items to them.

Read the full article here.