ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM
https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

January 13, 2021

ANNUAL INTELLECTUAL PROPERTY REPORT TO CONGRESS

Executive Office of the President of the United States | January 2021

This report is submitted pursuant to 15 U.S.C. §8114.

During the past four years, President Trump and his Administration have worked to promote strong intellectual property rights protection and enforcement, both domestically and abroad. As part of an integrated approach, the Trump Administration views our intellectual property strategy, policy and enforcement efforts, together, as key to helping secure the future of our innovative economy and to maintaining our competitive advantage.

The Trump Administration's Annual Intellectual Property Report to Congress, developed by the Office of the U.S. Intellectual Property Enforcement Coordinator, brings together the combined and coordinated efforts of the White House, the Departments of Commerce, Justice, Homeland Security, State, Treasury, Defense, Health and Human Services, and Agriculture, the Office of the U.S. Trade Representative, and the U.S. Copyright Office. This report was originally mandated to be submitted by the U.S. Intellectual Property Enforcement Coordinator over a decade ago by the Prioritizing Resources and Organization for Intellectual Property Act of 2008, and builds upon that framework to provide an overview of the Trump Administration's intellectual property enforcement strategy and policy efforts. For the United States' approach to intellectual property and innovation policy to be successful, it must continue to be a combined effort that includes all branches of government, the private sector, and our international partners.

The Trump Administration continues to build on past strategic efforts in all areas of intellectual property policy, including patents, copyrights, trademarks and trade secrets, both domestically and abroad. But the Administration also recognizes that for the United States to maintain its future economic competitiveness, we need to think strategically and shift the paradigm to one where we not only place America First, but regard America's inventive and creative capacity as something that we must protect, promote and prioritize.

Read the full report here.

DHS STRATEGIC ACTION PLAN TO COUNTER THE THREAT POSED BY THE PEOPLE'S REPUBLIC OF CHINA

U.S. Department of Homeland Security Office of Strategy, Policy, and Plans | January 12, 2021

Though the global security environment has evolved considerably since the Department of Homeland Security's (DHS) founding, its fundamental mission has endured: To safeguard the Homeland, its values, and the American way of life. The changing geopolitical landscape, led by the return of great power competition, is nowhere more evident than in the People's Republic of China's (PRC) ascension to the world-stage. For decades, marked by Beijing's symbolic entry in the World Trade Organization (WTO), the PRC has leveraged non-traditional tools to gain access to and exploit our global institutions and rules-based order, with little to no response. This has resulted in the erosion of, and direct attacks against, U.S. national security and economic competitiveness, including the exploitation of our immigration system manipulation of open-markets, and theft of our intellectual property. Under this Administration, the PRC's threat to the Homeland is now being appropriately prioritized and met with a resolute commitment to safeguard America. As denoted in the 2017 National Security Strategy of the United States (NSS) and 2020 United States Strategic Approach to the PRC (Strategic Approach), DHS and the broader United States Government (USG) have entered into a period of sustained competition against the PRC, requiring continued attention, adaptation, and resourcing to safeguard the American people and Homeland. The American people rely on DHS to play an integral role in the USG's competition with the PRC. The more than 240,000 men and women of the Department stand ready to curb malign PRC activity and the myriad of other challenges. This study, which seeks to more strategically identify, assess, and leverage the Department's unique resources and authorities, reflects these efforts. The DHS China Strategic Action Plan (SAP) is informed by and nests within the NSS and the Strategic Approach, which delineate the United States' strategic approach to PRC through the pursuit of four goals: (1) protecting the American people, the Homeland, and the American way of life; (2) promoting American prosperity; (3) preserving peace through strength; and (4) advancing American interests.

Read the full report here.

PUTTING MONEY IN THE PARTY'S MOUTH: HOW CHINA MOBILIZES FUNDING FOR UNITED FRONT WORK

Ryan Fedasiuk | CSET | January 11, 2021

Over the past two years, a series of government and think tank reports have shed light on the united front, the collection of organizations the Chinese Communist Party (CCP) leverages to co-opt non-Party institutions and influence minority groups at home and overseas (USCC, August 2018; ASPI, June 2020). Facing heightened scrutiny, People's Republic of China (PRC) officials have repeatedly insisted that there is "no factual basis" to Western reporting on China's influence operations, and accused foreign analysts of "maliciously hyping up the normal foreign exchanges of the United Front Work Department" (MFA, June 2020; PRC Embassy in Sweden, August 2019). However, there is a universal truth known to government bureaucrats in every country: budgets speak louder than words. As this paper demonstrates, the scale and scope of funding for the united front system belie the Chinese government's claims about its importance and function. This article synthesizes information from more than 160 budget and expense reports from national and regional PRC government and Communist Party entities. [1] It finds that organizations central to China's national and regional united front systems spent more than $2.6 billion in 2019, exceeding funding for China's Ministry of Foreign Affairs (MFA, 2020). [2] Nearly $600 million (23 percent) was set aside for offices designed to influence foreigners and overseas Chinese communities.

Read the full article here.

COMPENDIUM OF RECOMMENDATIONS ON CHINA POLICY FOR THE BIDEN ADMINISTRATION

Wilson Center | January 8, 2021

In recent years, U.S.-China relations have become increasingly competitive, with areas of confrontation rapidly expanding at the expense of traditional areas of cooperation. The incoming Biden administration must address this hostile climate with new thinking that realistically assesses threats to national security while remaining open to opportunities for further engagement with China to revitalize this crucial bilateral relationship. The Wilson Center and the U.S.-China Business Council have jointly created the Compendium of Recommendations on China Policy for the Biden Administration to renew the national debate and help the incoming administration navigate the policy options at its disposal. Neither Wilson Center nor the U.S.-China Business Council claim ownership of the materials provided herein and nor do they necessarily endorse the perspectives provided. Each item is compiled impartially with the aim of broadening foreign policy discussions and charting a new direction for American diplomacy. It is our goal that this platform will become a point of reference for policymakers and the general public alike. Neither Wilson Center nor the U.S.-China Business Council claim ownership of the materials provided herein and nor do they necessarily endorse these perspectives.

Read the full article here.

FOR CHINESE FIRMS, THEFT OF YOUR DATA IS NOW A LEGAL REQUIREMENT

Bradley Thayer | The Hill | January 7, 2021

In late December, the Department of Homeland Security (DHS) released a significant but largely overlooked advisory to American businesses, warning of the risks associated with the use of data services and equipment from firms with ties to the People's Republic of China. The advisory noted that this presents a major threat to data security for the U.S. government, businesses and people, because China will have the ability to access data covertly through entities it influences or controls. The advisory highlights the persistent risk of Chinese government-sponsored data theft because of newly enacted Chinese laws — specifically, the National Intelligence Law of 2017, Data Security Law of 2020, and Cryptology Law of 2020. These laws compel Chinese businesses and citizens — including through academic institutions, research service providers, and investors — to support and facilitate China's government access to the collection, transmission and storage of data.

Read the full article here.

BIDEN'S DAY 1 RUSSIA PROBLEM

Jack Devine | The Hill | January 11, 2021

After a half-century of closely observing how our adversaries surreptitiously collect intelligence on the United States and our friends across the globe, few espionage operations trouble me more than the recent Russian cyber attack on our federal agencies. Not only is this one of the largest and most potentially damaging hacks of all time, but it represents a dangerous escalation in the spy v. spy struggle in which the intelligence world has engaged for decades. How President-elect Biden responds will complicate his opening days and possibly define his legacy. The outlines of the Russian attack are starting to reveal themselves and serve as a wake-up call for all. As the U.S. Cybersecurity and Infrastructure Security Agency has warned, hackers who pose "a grave risk to the federal government" attacked the SolarWinds IT management software suite in March 2020.

Read the full article here.

WHAT THE COLD WAR CAN TEACH WASHINGTON ABOUT CHINESE TECH TENSIONS

Brendan Thomas–Noone | Brookings Tech Stream | January 12, 2021

In a 1982 speech, then-U.S. Secretary of Defense Caspar W. Weinberger warned that the United States had for the better part of a decade facilitated unfettered technological transfer and trade with the Soviet Union. This high-tech transfer, the secretary argued, was being done through "legal and illegal channels" and was effectively the technological "rope to hang us," as it was bolstering Soviet military capability. Replace the Soviet Union with China, and the themes of Weinberger's speech would not seem out of place today. At the time, a strategic competitor appeared to be rapidly advancing on U.S. technological superiority through a concerted campaign of technology transfer, aided by U.S. scientific engagement policies, an open academic system, and intellectual property theft. In some cases, this had been abetted by U.S. high-tech trade with the Soviets over the previous decade: The sale of advanced ball bearing machines had helped improve the accuracy of Soviet missiles, the Pentagon chief declared. In other cases, allies were to blame, as when Japan sold civilian dockyards to the USSR that were diverted to service the Soviet's new aircraft carriers. Replace ball bearings with lasers and dry docks for semiconductor manufacturing equipment, and Weinebrger could be speaking of today's trade tensions between the United States and China.

Read the full article here.

US RAISES CONCERN OVER CHINA, RUSSIA TARGETING COVID -19 VACCINE SUPPLY CHAIN

Mint | January 13, 2021

As countries are either in the process of administrating Covid -19 vaccines or are gearing up to do so, the director of the National Counterintelligence and Security Center (NCSC), has raised concerns over the efforts by China and Russia to target the vaccine supply chain. Speaking during a virtual event hosted by The Washington Post, the NCSC top official William Evanina said, "It's a very complex problem, and I would definitely commend the women and men of the Army and the entire government that is part of Operation Warp Speed to ensure that we are able to facilitate that transportation of the vaccine safely full well knowing our adversaries are trying to disrupt that supply chain."

Read the full article here.

WHY THE LATEST CYBERATTACK WAS DIFFERENT

Robert Muggah | Foreign Policy | January 11, 2021

All during 2020, as the coronavirus pandemic swept around the world, another novel virus with devastating long-term effects spread unnoticed worldwide. Sometime in late 2019 or early 2020, at least one group of advanced hackers inserted malware into network software supplied by SolarWinds, a maker of information technology infrastructure software based in Austin, Texas. The decision to target SolarWinds looks strategic given the company's vast U.S. and global clientele in the public, private, and nonprofit sectors. Publicly exposed in December 2020, the infectious malware—dubbed Sunburst by the cybersecurity firm FireEye and Solorigate by Microsoft—may turn out to be the most audacious cyberespionage campaign in history. For months, attackers stealthily infiltrated governments and businesses via a Trojan horse-style update to SolarWinds' Orion cybersecurity management software. Like the coronavirus, Sunburst and another recently discovered piece of malware reveal the downside of global connectivity and the failure of global cooperation to deal with contagion.

Read the full article here.

FBI WARNS OF CYBERATTACKS TO DISTANCE LEARNING

Luke Barr | ABC News | January 4, 2021

As students head back to the classroom after the holidays, the FBI is warning students, teachers and parents that cyber criminals and bad actors are looking to exploit online classrooms. FBI Cyber Section Chief Dave Ring told ABC News the agency has seen an uptick in ransomware attacks. "It's of greater concern now when it comes to K-12 education, because so many more people are plugged into the technology with schooling because of the distance learning situation," he said. "So things like distributed denial of service attacks, even ransomware and of course, domain spoofing, because parents are interacting so much more with the schools online." In early December, the FBI and the Cybersecurity and Infrastructure Security Agency issued a warning that showed a nearly 30% increase in ransomware attacks against schools. "In August and September, 57% of ransomware incidents reported to the MS-ISAC involved K-12 schools, compared to 28% of all reported ransomware incidents from January through July," the alert said.

Read the full article here.

IN U.S. BACKYARD: HOW CHINA EMBEDDED ITSELF IN CANADA

Cleo Paskal | Sunday Guardian Live | January 2, 2021

Canada has been making headlines in India recently, and not in a good way. There were Prime Minister Justin Trudeau's statements about the farmer issue, seen in New Delhi as interference in internal affairs. And then documents were released showing that as late as 2018 Canada was allowing PLA soldiers to observe Canadian winter warfare training, seen as of use to China in its aggression against India in the Himalayas—and when the Canadian military unilaterally decided to stop the training, some in Canadian foreign affairs hit the roof. This has raised questions about Canada's foreign policy, and in particular, its relations with China. The questions are legitimate. To answer them, it helps to look at three factors that helped shape the early development of China/Canada relations: missionaries, leftist sympathies combined with anti-Americanism, and the business community.

Read the full article here.

WHEN DO U.S. COMPANIES AND INSTITUTIONS NEED TO BE CONCERNED ABOUT NATIONAL SECURITY?

Nick Oberheiden | JD Supra | January 6, 2021

In today's world, companies in various industries are increasingly running into issues that have national security implications. Research universities and other academic institutions can face issues involving national security risks as well. As a result, whereas protecting national security was once a matter reserved for the federal government, today, both private and public companies and institutions can play vital roles, and these entities must implement adequate security controls to mitigate threats and prevent intrusions. Traditionally, protecting national security largely centered around protecting the nation's borders. If threats could not come in, then they could not cause harm. While border security remains a fundamental concern today (and this is an area in which businesses and universities can play a part), the ongoing technological revolution has forced the U.S. government as well as domestic businesses and universities to confront unprecedented challenges in a world that is constantly evolving.

Read the full article here.

U.S. PUBLISHES LIST OF CHINESE AND RUSSIAN FIRMS WITH MILITARY TIES

Karen Freifeld | Reuters | December 21, 2020

The Trump administration on Monday published a list of Chinese and Russian companies with alleged military ties that restrict them from buying a wide range of U.S. goods and technology. Reuters first reported last month that the U.S. Department of Commerce drafted a list of companies that it linked to the Chinese or Russian military, news that brought a rebuke from Beijing. The final list does not include Commercial Aircraft Corporation of China (COMAC), or the Hong Kong subsidiaries of Colorado's Arrow Electronics and Texas-based TTI Inc, a Berkshire Hathaway electronics distributor. Those companies were on the draft list seen by Reuters. However, Shanghai Aircraft Design and Research Institute, which designs COMAC planes, and Shanghai Aircraft Manufacturing Co, which manufactures COMAC planes, are on the list. China urged the United States to stop what it called erroneous actions and treat all companies in an equal way, foreign ministry spokesman Wang Wenbin said at a daily news conference in Beijing on Tuesday.

Read the full article here.