



<https://asce.tamus.edu>

THE OPEN SOURCE MEDIA SUMMARY

April 14, 2021

ANNUAL THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY

Office of the Director of National Intelligence | April 9, 2021

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the FY21 Intelligence Authorization Act (P.L. 116-260). This report reflects the collective insights of the Intelligence Community (IC), which is committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world. This assessment focuses on the most direct, serious threats to the United States during the next year. The order of the topics presented in this assessment does not necessarily indicate their relative importance or the magnitude of the threats in the view of the IC. All require a robust intelligence response, including those where a near term focus may help head off greater threats in the future, such as climate change and environmental degradation. As required by the law, this report will be provided to the congressional intelligence committees as well as the committees on the Armed Services of the House of Representatives and the Senate. Information available as of 9 April 2021 was used in the preparation of this assessment.

Read the full article [here](#).

BIDEN'S NATIONAL SECURITY TEAM LISTS LEADING THREATS, WITH CHINA AT THE TOP

Greg Myre | NPR | April 13, 2021

The U.S. intelligence community said Tuesday that it views four countries as posing the main national security challenges in the coming year: China, followed by Russia, Iran and North Korea. "China increasingly is a near-peer competitor, challenging the United States in multiple arenas — especially economically, militarily, and technologically — and is pushing to change global norms," said the report released by the Office of the Director of National Intelligence. The report cites China's growing military assertiveness in several regional disputes, including Taiwan, the India-China border and the South China Sea. "China seeks to use coordinated, whole-of-government tools to demonstrate its growing strength and compel regional neighbors to acquiesce to Beijing's preferences, including its claims over disputed territory," the report says.

Read the full article [here](#).



CITING PRESSURE, UNH ENDS CONTRACT WITH CHINA-FUNDED CONFUCIUS INSTITUTE

Todd Bookman | NHPR | April 13, 2021

The University of New Hampshire is ending a partnership with the Confucius Institute, a controversial educational group funded by the Chinese government. Confucius Institutes operate at colleges and universities in the U.S., providing Chinese language classes as well as cultural and exchange programs, often at little or no cost to the universities. Critics including U.S. intelligence officials caution that the institutes function as propaganda arms of the Chinese Communist party. Citing rising pressure from Washington, UNH says it will end its partnership on July 30. "We made the difficult decision to close it due to amplified concerns in Washington about security and influence. The federal government has made it increasingly difficult for us to operate the Institute, including the real possibility of losing significant federal research funding if we do not close the institute," said Erika Mantz, a UNH spokesperson. UNH first partnered with the Institute in 2010, and renewed a five-year contract in 2019. The program has a modest presence on campus, including three language instructors and two study abroad programs to Chengdu, China, according to its website.

Read the full article [here](#).

CHINA'S MESSAGE TO AMERICA: WE'RE AN EQUAL NOW

Lingling Wei and Bob Davis | The Wall Street Journal | April 12, 2021

It quickly became obvious in Anchorage, Alaska, last month that Chinese President Xi Jinping's diplomatic envoys hadn't come carrying olive branches. Instead they brought a new world view. As Biden administration officials expected in their first meeting with Chinese counterparts, Yang Jiechi, Mr. Xi's top foreign-policy aide, and Foreign Minister Wang Yi asked them to roll back Trump-era policies targeting China. Beijing wanted to restore the kind of recurring "dialogue" Washington sees as a waste of time, say U.S. and Chinese officials briefed on the Alaska meeting. Mr. Yang also delivered a surprise: a 16-minute lecture about America's racial problems and democratic failings. The objective, say Chinese officials, was to make clear that Beijing sees itself as an equal of the U.S. He also warned Washington against challenging China over a mission Beijing views as sacred—the eventual reunification with Taiwan.

Read the full article [here](#).

HOUSE SCIENCE AND ARMED SERVICES COMMITTEE CHAIRS LOOK TO COLLABORATE WITH PRESIDENT BIDEN TO ADDRESS RISKS TO US RESEARCH ENTERPRISE

U.S. House of Representatives Committee on Science, Space, and Technology | April 12, 2021

Last Friday, Members of both the House Science, Space, and Technology Committee and House Armed Services Committee sent a letter to President Joe Biden expressing their interest in collaborating with the Administration on taking a measured and balanced approach to strengthen the security and integrity of the country's academic research enterprise. The letter was signed by Chairwoman Eddie Bernice Johnson (D-TX), Chairman Adam Smith (D-WA), Research and Technology Subcommittee Chairwoman Haley Stevens (D-MI), and Cyber, Innovative Technologies, and Information Systems Subcommittee Chairman Jim Langevin (D-RI). "We strongly support a measured and balanced approach to this issue, one that promotes research integrity and security without impeding academic freedom, international collaboration, and the global competition for talent, all of which are critical to our continued leadership in science and innovation," said the Chairs in the letter.

Read the full article [here](#).



THE U.S. GOVERNMENT NEEDS TO OVERHAUL CYBERSECURITY. HERE'S HOW.

Jonathan Reiber and Matt Glenn | Lawfare | April 9, 2021

After the 2015 hack of the U.S. Office of Personnel Management, the SolarWinds breach, and—just weeks after SolarWinds—the latest Microsoft breach, it is by now clear that the U.S. federal government is woefully unprepared in matters of cybersecurity. Following the SolarWinds intrusion, White House leaders have called for a comprehensive cybersecurity overhaul to better protect U.S. critical infrastructure and data, and the Biden administration plans to release a new executive order to this end. What should this reinvestment in cybersecurity look like? Although the United States is the home of many top cybersecurity companies, the U.S. government is behind where it should be both in technology modernization and in mindset. Best-in-class cyberdefense technologies have been available on the market for years, yet the U.S. government has failed to adopt them, opting instead to treat cybersecurity like a counterintelligence problem and focusing most of its resources on detection. Yet the government's massive perimeter detection technology, Einstein, failed to detect the SolarWinds intrusion—which lays bare the inadequacy of this approach.

Read the full article [here](#).

CHINA BUILDS ADVANCED WEAPONS SYSTEMS USING AMERICAN CHIP TECHNOLOGY

Ellen Nakashima and Gerry Shih | The Washington Post | April 9, 2021

In a secretive military facility in southwest China, a supercomputer whirs away, simulating the heat and drag on hypersonic vehicles speeding through the atmosphere — missiles that could one day be aimed at a U.S. aircraft carrier or Taiwan, according to former U.S. officials and Western analysts. The computer is powered by tiny chips designed by a Chinese firm called Phytium Technology using American software and built in the world's most advanced chip factory in Taiwan, which hums with American precision machinery, say the analysts. Phytium portrays itself as a commercial company aspiring to become a global chip giant like Intel. It does not publicize its connections to the research arms of the People's Liberation Army.

Read the full article [here](#).

BIDEN, CONGRESS ROLL OUT BIG PLANS TO EXPAND NATIONAL SCIENCE FOUNDATION

Jeffrey Mervis | Science | April 6, 2021

The idea of massively expanding the budget and mission of the National Science Foundation (NSF) to help the United States out-innovate China is gaining political momentum in Washington, D.C. In Congress, Senate Majority Leader Chuck Schumer (D-NY) is preparing to introduce a revised version of bipartisan legislation that would create a technology directorate at NSF and boost its funding by \$100 billion. The changes address fears voiced by academic leaders that the new unit might disrupt the agency's culture and dilute NSF's ability to support basic research at universities. On 31 March, President Joe Biden lined up behind the concept, including both the new directorate and a \$50 billion bump for NSF in his \$2.3 trillion proposal to upgrade the nation's aging infrastructure. And late last month, Representative Eddie Bernice Johnson (D-TX), chair of the science committee of the U.S. House of Representatives, also backed both a new directorate and a larger NSF budget as part of a bill reauthorizing programs at the agency, which currently has an \$8.5 billion budget.

Read the full article [here](#).



ARTIFICIAL INTELLIGENCE KEY TO MAINTAINING MILITARY, ECONOMIC ADVANTAGES, LEADERS SAY

David Vergun | U.S. Department of Defense News | April 9, 2021

Marine Corps Lt. Gen. Michael S. Groen, director of the Joint Artificial Intelligence Center, and Robert O. Work, vice chair of the NSCAI, spoke to reporters at the Pentagon. Work provided an overview of the report: The United States does not have a strategy, organizational structure and resources to win the competition with China for effective implementation of AI, he said. "So the first thing is we have got to do is to take this competition seriously, and we need to win it." To win, AI must receive the necessary funding, at least 3.4% of the DOD budget. Those funds should then be channeled into priority areas as recommended by a steering committee consisting of the deputy defense secretary, the vice chairman of the Joint Chiefs of Staff and the principal director of national intelligence, he said, noting that a good first step was having the JAIC report directly to the deputy defense secretary. That steering committee would also remove any bureaucratic obstacles and would oversee the development of a technology annex to the National Defense Strategy, Work said.

Read the full article [here](#).

US UNIVERSITIES CALL FOR CLEARER RULES ON SCIENCE ESPIONAGE AMID CHINA CRACKDOWN

Nidhi Subbaraman | Nature | April 6, 2021

The US government is converging on a long-awaited set of rules designed to protect American science from theft by foreign spies. A series of announcements this year describe steps that US universities and researchers must take when reporting foreign financing and collaborations to US science funders. But university groups say they need more clarity on how to implement the rules. And the guidelines do not spell out how institutions can address concerns of racial profiling sparked by the US government's crackdown on foreign interference in recent years. The issue of foreign influence and interference in US research has loomed large as geopolitical tensions between the United States and China have risen. The new guidelines date back to the last days of former US president Donald Trump's administration; so far, President Joe Biden's administration has not indicated that it will seek to change the policies and that it is open to feedback.

Read the full article [here](#).

DID CHINA CROSS A NEW RED LINE IN CYBERSPACE?

Mark Montgomery and Trevor Logan | Sunday Guardian Live | March 27, 2021

Did China cause the blackouts in Mumbai last year? Nearly six months later, the answer is still unclear, but if recent reports that a Chinese cyber operation bears partial responsibility are accurate, Beijing just signalled a willingness to use its cyber power to target civilian lifeline infrastructure during a crisis. Even more worrying, the hackers used hard-to-control cyberattack tools in a destructive manner against a nuclear-armed country, India. In a report last month, threat analysts at the cybersecurity firm Recorded Future detailed their discovery of China's systematic penetration of India's electricity infrastructure. Given the event's concurrence with the border skirmishes in the disputed area of Galwan Valley, the Chinese hackers appear to have targeted nodes of India's electric grid to demonstrate Beijing's capabilities and to convince New Delhi that it should not oppose China's claims over the area. Without analysis of the malware or confirmation from Indian officials, we will not know if malware was responsible for the Mumbai blackout, if the outage was caused by operator error while responding to the malware, or if the outage was some kind of combination of these.

Read the full article [here](#).



AN ALLIANCE OF AUTOCRACIES? CHINA WANTS TO LEAD A NEW WORLD ORDER.

Steven Lee Myers | The New York Times | March 29, 2021

President Biden wants to forge an “alliance of democracies.” China wants to make clear that it has alliances of its own. Only days after a rancorous encounter with American officials in Alaska, China’s foreign minister joined his Russian counterpart last week to denounce Western meddling and sanctions. He then headed to the Middle East to visit traditional American allies, including Saudi Arabia and Turkey, as well as Iran, where he signed a sweeping investment agreement on Saturday. China’s leader, Xi Jinping, reached out to Colombia one day and pledged support for North Korea on another. Although officials denied the timing was intentional, the message clearly was. China hopes to position itself as the main challenger to an international order, led by the United States, that is generally guided by principles of democracy, respect for human rights and adherence to rule of law. Such a system “does not represent the will of the international community,” China’s foreign minister, Wang Yi, told Russia’s, Sergey V. Lavrov, when they met in the southern Chinese city of Guilin.

Read the full article [here](#).

FIXING CRUMBLING U.S. INNOVATION INFRASTRUCTURE

Deborah Wince-Smith | Forbes | March 29, 2021

One of the biggest wake-up calls of the past year has been how flat-footed and unprepared we were as a nation to the global crisis of the Covid-19 pandemic. The United States has the capacity and resources to respond effectively to these types of challenges, yet we seem perpetually stunned when they happen and end up scrambling to adapt. We as a nation can no longer afford that kind of complacency. The very foundation of our economic prosperity is at stake and crumbling on our watch. To ensure the economic vitality, national security, and inclusive prosperity of the United States and its citizens, leaders in both the private and public sectors must work to create greater innovation capacity and resilience within our national infrastructure network. That means greater investment in our roads, bridges, mass transit, water supply lines, and power generation; it also means creating ubiquitous access to high-speed broadband and building out “5G and beyond” wireless connectivity. It also means investing in the United States research enterprise, including our universities and the National Laboratories — both of which couple world-class talent with globally unique tools and facilities.

Read the full article [here](#).

INVOLVE ACADEMICS IN CONFRONTING ACADEMIC FREEDOM ISSUES

Christopher Hughes | University World News | April 9, 2021

The targeting of European academics and think tanks by the Chinese state in March has given rise to much discussion about the impact of the internationalisation of higher education on academic freedom. Aside from expressions of support for the targeted individuals and organisations, however, there appear to be few substantial ideas on how academics can work together in a practical way to preserve the integrity and credibility of their profession. The threats to academic freedom are, of course, most conspicuous for academics working under autocratic regimes. Yet their colleagues in more open societies find themselves with little leverage for improving the situation when their own institutions fail to take a lead. This situation is becoming more precarious as plans by governments to impose solutions raise the prospect of a further erosion of institutional autonomy and going down the path of global decoupling that would be detrimental to all sides. It is to address these dilemmas that members of the Academic Freedom and Internationalisation Working Group (AFIWG) came together in 2019.

Read the full article [here](#).



COMMISSION SEEKS TO BLOCK CHINA FROM SENSITIVE JOINT SCIENCE PROJECTS

Cristina Gallardo | Politico | March 30, 2021

The EU is pressing China to agree to a list of conditions before allowing it to cooperate with European researchers on sensitive areas of research, but there are fears that tie-ups with Britain, Switzerland and Israel could also be prevented by the proposed rules. Since 2019, the EU and China have been negotiating an agreement aimed at boosting bilateral cooperation on research and innovation projects. Until now, cooperation has been limited to a number of areas where there was a strong joint interest, such as food security, agriculture and biotechnology. The European Commission now wants the Chinese government to sign up to rules on issues such as intellectual property, access to R&D funds, open access to published research, ethics, mobility of researchers, and reciprocity. But EU officials say they are frustrated at the slow progress, due to what they describe as an apparent reluctance on the Chinese side to accept these level playing-field rules. As a result, the Commission is pondering whether to leave sensitive areas of tech such as quantum science, artificial intelligence and 5G out. "The biggest stumbling block on the Chinese side is that they don't see the need to discuss the framework conditions," an EU official said. "We want to limit for the moment our cooperation to those sectors in which we think we can be safely cooperating."

Read the full article [here](#).

SOUTH CHINA TECH CAPITAL TARGETS TOP FOREIGN TALENT TO DRIVE REFORM

Wang Xintong | Caixin | April 8, 2021

The South China tech hub of Shenzhen has launched a three-year pilot program to attract high-level foreign talent, including top scientists and entrepreneurs, to help turn it into a global technology and innovation powerhouse. The program includes a set of standards implemented Tuesday to certify urgently needed high-end foreign talent in Shenzhen, the country's pioneer of reform and opening-up in the southern province of Guangdong, according to a notice (link in Chinese) issued by the city government. Such certifications had previously only been handled by the Guangdong government. Foreign talents who work in Shenzhen and successfully apply for certification can enjoy benefits such as a simplified application process (link in Chinese) for visas which will allow them to stay in China for up to 10 years, according to the State Administration of Foreign Experts Affairs. The new standards, divided into seven categories, require candidates to meet at least one of the conditions within the categories, such as participating in a previous China talent program, holding globally recognized professional qualifications, and scoring 85 or more points in the system which assesses foreigners' qualifications to apply for work permits, the notice said.

Read the full article [here](#).

SAFEGUARDING OUR FUTURE SECURE AMERICA'S FUTURE IN QUANTUM: PROTECT YOUR RESEARCH

National Counterintelligence and Security Center | April 6, 2021

Foreign adversaries are targeting America's quantum information science enterprise to gain economic and military advantage. In the cross-hairs are quantum industry and academic personnel, facilities, networks, research and technology. See the new "Safeguarding our Future" bulletin [here](#).

Read the full article [here](#).



UNIVERSITIES FEAR RESEARCHER PIPELINE IS UNDER THREAT

Yojana Sharma | University World News | April 8, 2021

With increasing global and regional competition for doctoral students to fuel expansion in technology-based industries, even top universities in Asia are beginning to worry about a continued pipeline of well-qualified students in STEM (science, technology, engineering and mathematics) areas as countries expand research in key areas such as artificial intelligence, quantum computing, genetics, nanotechnology, robotics and other areas. Global competition has been enhanced by the rivalry between China and the United States in technology, with the US also pressuring Europe and Japan to curb research with China that is deemed sensitive. For Asian countries attracting foreign STEM PhD students, the largest contingent has come from China. Countries such as Japan are already talking of more stringent vetting of PhD students from countries including China for more strategically sensitive PhD subjects, and having to rely on local students or foreign students from other countries in the region. At the same time Beijing has initiated a campaign to keep PhD students and young researchers at home as it expands in major STEM areas as part of its own recently announced drive for self-sufficiency in technology.

Read the full article [here](#).

INSIDER THREAT VS. INSIDER RISK: WHAT'S THE DIFFERENCE?

Sharon Shea | Tech Target | December 30, 2020

Insider threat, a long-used term in the infosec industry, is one Joe Payne is ready to retire. Its replacement? Insider risk. Payne's reasoning is that much "malicious" insider activity -- such as deleting, copying or uploading files to collaboration apps or cloud storage platforms -- is not a threat, per se, but a consequence of the collaboration culture spreading in today's enterprises. But that doesn't mean risky behavior can be ignored. "We're careful not to call them threats because they might not actually be threats at all; they might just be an indicator that something needs following up," said Payne, president and CEO of Code42 and co-author of *Inside Jobs*. Insider risk, Payne noted, may be even more challenging for enterprises to solve than the traditional insider threat. In this excerpt from Chapter 3 of *Inside Jobs*, published by Skyhorse Publishing, Payne and co-authors Jadee Hanson and Mark Wojtasiak explain the various insider risk profiles common in collaboration culture and how even well-meaning employees may present security indicators that warrant further investigation.

Read the full article [here](#).

THE TEXAS A&M UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.

<https://rso.tamug.edu>

