ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

January 19, 2022

THE PENTAGON'S NEW CYBERSECURITY MODEL IS BETTER, BUT STILL AN INCREMENTAL SOLUTION TO A BIG CHALLENGE

Dr. Georgianna Shea | Federal News Network | January 17, 2022

The Pentagon announced in November a new "strategic direction" for its Cyber Maturity Model Certification, calling it CMMC 2.0 and essentially admitting the first iteration was overly complex and costly. The new version better aligns to existing federal standards and requirements but falls well short of being the "bold change" President Biden called for in his much-touted May cybersecurity executive order. Prior to the creation of CMMC, federal acquisition regulations required all defense contractors that interacted with controlled unclassified information (CUI) to implement the basic cyber hygiene safeguards listed in the National Institute of Standards and Technology guidelines, NIST Special Publication (SP) 800-171. Companies would then conduct self-assessments of their compliance. Predictably, not all companies assessed themselves equally or honestly, or addressed the issues they self-identified. In November 2020, after nearly two years of development, the Defense Department introduced the original CMMC. Its most significant change was a new requirement that a third-party conduct the assessment for all organizations seeking contracts, including universities applying for grants.

Read the full article here.

STRENGTHENING SCIENTIFIC INTEGRITY

Alondra Nelson and Jane Lubchenco | Science | January 11, 2022

A robust democracy requires a common wellspring of reliable information. During his first days in office, US President Biden affirmed that evidence-based decision-making—informed by vigorous science and unimpeded by political interference—would be a pillar of his administration. He directed ambitious actions to implement that goal, including the creation of an interagency Scientific Integrity Task Force, which has just released the first-ever, comprehensive assessment of scientific integrity policy and practices in the US government. The task force included 48 scientists, statisticians, engineers, lawyers, and policy-makers with a diversity of experiences from 29 federal agencies, and it received input from hundreds of outside experts from academia, the nonprofit sector, industry, and the public. The group found that although federal agency science is generally sound—that is, reported violations of scientific integrity policies are small in number compared to the magnitude of the federal scientific enterprise—there have been lapses that could undermine public trust in science and jeopardize federal scientists' and technologists' morale and motivation to innovate.

Read the full article here.

PROTECTING FEDERAL RESEARCH FROM FOREIGN INFLUENCE

U.S. Government Accountability Office | January 11, 2021

Federally-funded researchers may face conflicts of interest if they receive funding or other benefits from foreign entities, which may be looking to gain access to that research. One such example was highlighted in May 2020, when a former researcher at a prominent U.S. university pleaded guilty to filing a false tax return that did not include hundreds of thousands of dollars in foreign income from a Chinese-government talent recruitment program. This Chinese program provides U.S. researchers with salaries and other benefits in exchange for sharing their research findings with China. This case is just 1 example of how foreign influence can be used to divert U.S. research to other countries. And with the U.S. government spending a reported $42 billion on university science and engineering research in fiscal year 2018, safeguarding this work is critical. In today's WatchBlog, we take a closer look at our report on federal conflict of interest policies and how they may help agencies prevent undue foreign influence in federally funded research. Researchers who get federal funding have to watch out for 2 kinds of conflict of interest: financial and non-financial.

Read the full article here.

HOW COUNTRIES ARE LEVERAGING COMPUTING POWER TO ACHIEVE THEIR NATIONAL ARTIFICIAL INTELLIGENCE STRATEGIES

Samar Fatima, Gregory S. Dawson, Kevin C. Desouza, and James S. Denford | Brookings
January 12, 2022

Using finely tuned hardware, a specialized network, and large data storage, supercomputers have long been used for computationally intense projects that require large amounts of data processing. With the rise of artificial intelligence and machine learning, there is an increasing demand for these powerful computers and, as a result, processing power is rapidly increasing. As such, the growth of AI is inextricably linked to the growth in processing power of these high-performing devices. Supercomputers aren't new. The term appeared in the late 1920s and the CDC 6600 (released in 1964) is generally considered to be the first true supercomputer. Early supercomputers used only a few extremely powerful processors but, in the late 1990s, computer experts realized that stringing together thousands of off-the-shelf processors would yield the greatest processing power. Current state-of-the-art supercomputers have over 60,000 massively parallel processors to approach petaflop performance levels.

Read the full article here.

WHAT CHARLES LIEBER'S CONVICTION MEANS FOR SCIENCE

Andrew Silver | Nature | January 18, 2022

Next week will mark two years since Harvard University chemist and nanotechnology pioneer Charles Lieber was arrested on allegations of lying to US federal authorities about his financial ties to China. Last month, a jury convicted him of making false statements, as well as related tax offences. Researchers say that the high-profile US criminal case is already having an impact on the scientific community. It marks the second time an academic researcher has been tried on accusations of hiding ties to China since the US Department of Justice (DOJ) launched its controversial 'China Initiative' to root out threats to national security. "I think it makes clear to academic researchers the importance of fully and honestly disclosing the research funding they're getting from sources to federal agencies when they're applying for awards," says Tobin Smith, vice-president for science policy and global affairs at the Association of American Universities in Washington DC, of which Harvard — in Cambridge, Massachusetts — is a member. "Transparency is critical to ensuring the integrity of scientific research."

Read the full article here.

U.S. PROSECUTORS RECOMMEND DROPPING CASE AGAINST MIT PROFESSOR OVER CHINA TIES -SOURCE

Nate Raymond | Reuters | January 14, 2022

Prosecutors have recommended that the U.S. Justice Department drop charges against a Massachusetts Institute of Technology professor accused of concealing his ties to China when seeking federal grant money, a person familiar with the matter said Friday. Federal prosecutors in Boston decided to seek dismissal of the case against Chinese-born mechanical engineer and nanotechnologist Gang Chen. It was the latest setback for a crackdown on Chinese influence within U.S. research. Boston prosecutors recommended the case's dismissal in recent weeks based on new information, the person said, adding the Justice Department has not made a final decision. He was accused of failing to disclose, among other things, that he served as an "overseas expert" to the Chinese government and sat on the advisory board of Shenzhen's Southern University of Science and Technology, or SUSTech, when applying for a U.S. Department of Energy grant. But Brian Kelly, a lawyer for Chen at Nixon Peabody, has said last week that "nothing significant was omitted on his application and several of the government's allegations were simply wrong."

Read the full article here.

CHINESE INFLUENCE OPERATIONS

Paul Charon and Jean-Baptiste Jeangène Vilmer | Strategic Research Institute of the Military School October 2021

For a long time, it could be said that China, unlike Russia, sought to be loved rather than feared; that it wanted to seduce and project a positive image of itself in the world, or to inspire admiration. Today, Beijing has not renounced to seduce, nor its overall attractiveness and its ambition to shape international standards, and it is essential for the Chinese Communist Party not to lose face. And yet, Beijing is also increasingly comfortable with infiltration and coercion: its influence operations have become considerably tougher in recent years and its methods are resembling more closely the ones employed by Moscow. This is a “Machiavellian turn” inasmuch as the Party-State now seems to believe that “it is much safer to be feared than to be loved,” in the words of Machiavelli in The Prince. This is a clear Russification of Chinese influence operations. This report delves into this evolution, with the ambition to cover the whole specter of influence, from the most benign (public diplomacy) to the most malign methods, that is, interference (clandestine activities).

Read the full article here.

MI5 WARNING OVER 'CHINESE AGENT' IN PARLIAMENT

Gordon Corera & Jennifer Scott | BBC News | January 14, 2022

An alert from the security service said Christine Ching Kui Lee "established links" for the Chinese Communist Party (CCP) with current and aspiring MPs. She then gave donations to politicians, with funding coming from foreign nationals in China and Hong Kong. It comes after a "significant, long-running" investigation by MI5, Whitehall sources told the BBC. One of the MPs funded by Ms Lee was Labour's Barry Gardiner, who received over £420,000 from her in five years - but he said he had always made the security services aware of the donations. Liberal Democrat leader Sir Ed Davey also received a £5,000 donation when he was energy secretary - but he said the money was accepted by his local association and it was "the first time he has been given cause to be concerned". But she said the UK has measures in place "to identify foreign interference". The security service said anyone contacted by Ms Lee should be "mindful of her affiliation" and its "remit to advance the CCP's agenda".

Read the full article here.

SECURING THE DEFENSE INDUSTRIAL BASE

Office of the Under Secretary of Defense for Acquisition & Sustainment | 2022

To safeguard sensitive national security information, the Department of Defense (DoD) launched CMMC 2.0, a comprehensive framework to protect the defense industrial base from increasingly frequent and complex cyberattacks. With its streamlined requirements, CMMC 2.0: cuts red tape for small and medium sized businesses, sets priorities for protecting DoD information, reinforces cooperation between the DoD and industry in addressing evolving cyber threats. Together, these enhancements will ensure accountability for companies to implement cybersecurity standards while minimizing barriers to compliance with DoD requirements, instill a collaborative culture of cybersecurity and cyber resilience, and enhance public trust in the CMMC ecosystem, while increasing overall ease of execution. "CMMC 2.0 will dramatically strengthen the cybersecurity of the defense industrial base," said Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy. "By establishing a more collaborative relationship with industry, these updates will support businesses in adopting the practices they need to thwart cyber threats while minimizing barriers to compliance with DoD requirements."

Read the full article here.

FOREIGN STUDENTS LOSE HOPE OF RETURN AMID COVID OUTBREAKS

Mimi Leung | University World News | January 14, 2022

With universities shut down and transport curtailed in a number of cities, the outlook has darkened for international students shut out of China since March 2020 who were hoping to return. The spread of the highly contagious Omicron coronavirus variant in China, particularly from the northern port city of Tianjin to central Henan province has led to a hardline government zero-COVID policy and new city lockdowns to curb the virus. Many hoped border restrictions would be eased by February as Beijing holds the Winter Olympic Games beginning on 4 February. An initial batch of international students, those enrolled at two Sino-US joint venture universities – Duke Kunshan University in Jiangsu province close to Shanghai, and New York University Shanghai – who have been stranded abroad since January 2020, had been told in November to prepare to return but wait for the go-ahead. But those hopes and the hopes of all international students are now receding, with major outbreaks in a number of cities, including Xian, Shenzhen near the border with Hong Kong, the eastern port city of Ningbo, and the major port city of Tianjin just 80 miles from Beijing.

Read the full article here.

WHY CAN'T CANADA CONVICT ANY CHINESE SPIES?

Julian Spencer-Churchill | iPolitics | January 17, 2022

The most recent Canadian failure to convict alleged Chinese agents is undermining American confidence that Canada won't be a sanctuary for foreign spies. The U.S. has let it be known that it expects an updated China policy from Ottawa soon, particularly one for domestic security. According to the director of the FBI, half of the agency's 5,000 active counterintelligence cases in the U.S. concern China, and one case is added every 10 hours. Chinese espionage costs the country US$225 billion to US$600 billion a year. Wikipedia lists 33 convictions of people in the U.S. spying for China, of which three-quarters are ethnically Chinese. The CSIS–RCMP Sidewinder operation revealed that Canada has been a target of Chinese espionage for decades. Although Public Safety Canada reported that eight Chinese were refused entry into Canada in 2020, the RCMP has never convicted anyone of stealing secrets in Canada on China's behalf.

Read the full article here.

UNIVERSITY TALENT 'BONANZA' FROM CRACKDOWN ON TECH FIRMS

Yojana Sharma | University World News | January 15, 2022

Universities in China and overseas are unexpectedly benefiting from China's crackdown on technology companies in recent months, with some top-level artificial intelligence (AI) and other high-end tech talent returning to academia as the sector shrinks and salaries are reined in. China is in the throes of a regulatory crackdown on its previously untouchable tech giants, clamping down on what is seen as their market-distorting practices. In April 2021, e-commerce giant Alibaba Group froze pay for senior executives while giving junior staff bigger salary increases at a time when Alibaba was a focus of the government crackdown fuelled by government concern about their market dominance and ability to sway public opinion. Last year, Alibaba was fined a record US$2.75 billion for alleged market competition violations.

Read the full article here.

CYBER ESPIONAGE CAMPAIGN TARGETS RENEWABLE ENERGY COMPANIES

Bill Toulas | Bleeping Computer | January 17, 2022

A large-scale cyber-espionage campaign targeting primarily renewable energy and industrial technology organizations have been discovered to be active since at least 2019, targeting over fifteen entities worldwide. The campaign was discovered by security researcher William Thomas, a Curated Intelligence trust group member, who employed OSINT (open-source intelligence) techniques like DNS scans and public sandbox submissions. Thomas' analysis revealed that the attacker uses a custom 'Mail Box' toolkit, an unsophisticated phishing package deployed on the actors' infrastructure, as well as legitimate websites compromised to host phishing pages. Most of the phishing pages were hosted on "*.eu3[.]biz", "*.eu3[.]org", and "*.eu5[.]net" domains, while the majority of the compromised sites are located in Brazil ("*.com[.]br").

Read the full article here.

BENCHMARKING CRITICAL TECHNOLOGIES

Kitsch Liao, Dr Samantha Hoffman and Karly Winkler | Australian Strategic Policy Institute
November 30, 2021

Technology policy formulation has recently gained a renewed importance for governments in the era of strategic competition, but contextual understanding and expertise in deciding where to focus efforts are lacking. As a result, decision-makers might not understand their own national strengths and weaknesses. It's difficult to judge whether a country's R&D outputs, no matter how advanced, and its development of production capacity, no matter how significant, align with the country's intended strategic objectives or can be used effectively to achieve them. The ability to measure the relative strengths and weaknesses of a country by weighing specific strategic objectives against technical achievements is of paramount importance for countries.

Read the full article here.