ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

February 23, 2022

JUSTICE DEPARTMENT SHUTTERS CHINA INITIATIVE, LAUNCHES BROADER STRATEGY TO COUNTER NATION-STATE THREATS

Ellen Nakashima | The Washington Post | February 23, 2022

The Justice Department is shuttering its controversial China Initiative and replacing it with a broader strategy aimed at countering espionage, cyberattacks and other threats posed by a range of countries, a top official said Wednesday. Assistant Attorney General Matthew G. Olsen, who heads the department's national security division, said the move was spurred by a growing recognition that the initiative's name and approach unintentionally fueled a "harmful perception" that the program unjustly targeted ethnic Chinese for prosecution. "I want to emphasize my belief," he said in a speech at George Mason University in Northern Virginia, just outside Washington, "that the department's actions have been driven by genuine national security concerns. But by grouping cases under the China Initiative rubric, we helped to" create a misperception. "It's important to end that perception," Olsen, who undertook a review of the program in November at the direction of Attorney General Merrick Garland, said in remarks to reporters before the speech.

Read the full article here.

WHITE HOUSE RECOGNIZES HYPERSONICS, DIRECTED ENERGY AS CRITICAL TECHNOLOGIES

Courtney Albon | C4ISRNET | February 8, 2022

The White House has added five new technology areas to its list of critical and emerging technologies — including hypersonic capabilities, directed energy, renewable energy generation and storage, nuclear energy and financial technology. The list of critical and emerging technologies, or CETs, was released Tuesday by the National Security Council and the National Science and Technology Council's Fast Track Action Subcommittee on Critical and Emerging Technologies. The update follows — and closely reflects — the key technologies included in the Pentagon's new science and technology vision, which was signed Feb. 1 by Under Secretary of Defense for Research and Engineering Heidi Shyu. It also comes just days after top Pentagon leaders convened a meeting with defense industry executives to discuss the importance of moving quickly to field hypersonic technology. The CET list is not meant to be a strategy but will inform a future strategy for U.S. technological competitiveness and national security, the report notes. It also serves as a resource to "promote U.S. technological leadership" and for cooperation with international allies. Within each CET, the report highlights core technologies or subfields.

Read the full article here.

NIH ISSUES A SEISMIC MANDATE: SHARE DATA PUBLICLY

Max Kozlov | Nature | February 16, 2022

The data-sharing policy could set a global standard for biomedical research, scientists say, but they have questions about logistics and equity. In January 2023, the US National Institutes of Health (NIH) will begin requiring most of the 300,000 researchers and 2,500 institutions it funds annually to include a data-management plan in their grant applications — and to eventually make their data publicly available. Researchers who spoke to Nature largely applaud the open-science principles underlying the policy — and the global example it sets. But some have concerns about the logistical challenges that researchers and their institutions will face in complying with it. Namely, they worry that the policy might exacerbate existing inequities in the science-funding landscape and could be a burden for early-career scientists, who do the lion's share of data collection and are already stretched thin. The mandate, in part, aims to tackle the reproducibility crisis in scientific research. Last year, a US$2-million, eight-year attempt to replicate influential cancer studies found that fewer than half of the assessed experiments stood up to scrutiny.

Read the full article here.

U.S. SCIENTIFIC RESEARCH AGENCIES TIGHTEN FOREIGN AFFILIATION RULES

Gopal Ratnam | Roll Call | February 15, 2022

U.S. research institutions and universities are gearing up to implement steps announced last month by the Biden administration to ensure that scientists seeking federal grants are not beholden to foreign governments or interests. The White House National Science and Technology Council issued a set of guidelines in January designed to ensure that scientists seeking federal grants do not have conflicts of interest stemming from their participation in foreign talent recruitment programs. The guidelines address a presidential national security memorandum issued in early 2021. That memorandum required any research institution receiving more than $50 million in federal science and technology grants in a year to certify that it has a research security program that can identify conflicts of interests. The 2021 Pentagon policy measure required all U.S. federal research agencies to obtain from applicants their current sources of funding, both domestic and foreign.

Read the full article here.

THE RISE OF VOICE CLONING AND DEEPFAKES IN THE DISINFORMATION WARS

Jennifer Kite-Powell | Forbes | September 21, 2021

In 2020, it was estimated that disinformation in the form of fake news costs around $78 billion annually. But deepfakes, mainly in social media, have matured and are fueled by the sophistication of artificial intelligence are moving into the business sector. In 2019, Deeptrace, a cybersecurity company reported that the number of online deepfake videos doubled, reaching close to 15,000 in under a year. Several startups like Truepic, that's raised $26 million from M12, Microsoft's venture arm, has taken a different approach to deepfakes. They focus on identifying not what is fake, tracking the authenticity of the content at the point it is captured. Yancho Yanchev, a data protection specialist and solicitor in the UK, says that deep fakes using real or faked images of others can fall under the scope of Global Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and similar rules across the globe. Yanchev says that this is especially true if those images are distributed for commercial or ideological purposes.

Read the full article here.

BIDEN MAKES TWO INTERIM APPOINTMENTS TO REPLACE TOP SCIENCE ADVISER

David Matthews | Science|Business | February 17, 2022

The White House has confirmed two temporary replacements for the outgoing presidential science adviser Eric Lander, as it seeks to reassure the community that his departure will not derail the administration's science agenda. Francis Collins, the long-serving National Institutes of Health director who retired last year, will step in as science adviser to the president. He will also co-chair a White House advisory body, the President's Council of Advisers on Science and Technology. Meanwhile, Alondra Nelson, a sociologist who is currently deputy director for science and society in the White House Office of Science and Technology Policy (OSTP), will for now take over as director. Lander, who occupied both roles, resigned earlier this month after reports that he bullied his subordinates. The two appointments came unusually fast – for Washington – and seemed aimed at reaffirming Biden's campaign pledges to take science more seriously than his predecessor.

Read the full article here.

U.S. CHARGES CHINESE COMPANY HYTERA WITH CONSPIRING TO STEAL TECH

Nikkei Asia | February 8, 2022

The U.S. Justice Department said on Monday it has brought criminal charges against China-based telecommunications company Hytera, accusing it of conspiring with former Motorola Solutions Inc employees to steal the American company's digital mobile radio technology. In a partially redacted indictment unsealed in Chicago, the government said Shenzhen-based Hytera Communications Corp recruited Motorola employees to steal proprietary trade data about the radios, known as walkie-talkies. The indictment charges Hytera by name, but it redacts the names of other co-defendants in the case, at least some of whom are the former Motorola employees the Chinese company is accused of recruiting. The indictment said Hytera recruited Motorola employees from 2007 through 2020, and that these workers received higher salaries and benefits than what they received at Motorola in exchange for stealing the trade secrets.

Read the full article here.

HOUSE PASSES COMPETES ACT, SETTING UP NEGOTIATIONS WITH SENATE

Mitch Ambrose | American Institute of Physics | February 4, 2022

The House passed the America COMPETES Act of 2022 today on a nearly party-line vote of 222 to 210, with Reps. Adam Kinzinger (R-IL) and Stephanie Murphy (D-FL) breaking ranks to respectively vote for and against it. The nearly 3,000-page legislative package is the House's response to the U.S. Innovation and Competition Act (USICA), which the Senate passed last year on a bipartisan vote of 68 to 32. Lawmakers will soon form a conference committee to negotiate a compromise bill that can garner enough support to pass both chambers. Among its core science provisions, the COMPETES Act sets ambitious targets for ramping up the budgets of the National Science Foundation, Department of Energy Office of Science, and National Institute of Standards and Technology. It also updates policy across those agencies, aiming to reinforce and expand on their existing research programs. In addition, the COMPETES Act seeks to bolster U.S. industry by directly providing $52 billion for domestic semiconductor R&D and manufacturing, and by recommending that Congress appropriate $45 billion for a new program to bolster domestic supply chains for critical goods.

Read the full article here.

ADVANCED PERSISTENT THREATS – DEFENDING AGAINST THESE CYBER ATTACKERS

Ron Kness | ClearanceJobs | February 18, 2022

For those not familiar with Advance Persistent Threats (APTs), they are a form of malware that can persist and do what they were programmed to do in a computer network for months or even years undetected. For example in March 2014, the U.S. Computer Emergency Response Team notified OPM of a breach with data stolen. And while the Response Team was able to remove the malware responsible for the first breach once they found it, a second piece of malware went undetected for a considerable amount of time. Between the two malwares, hackers made off with 4.2 million records of federal employees that included personnel files, security clearance background information and more than 5 million fingerprint records. The intruder believed responsible for planting the malware (and installing a back door to the network) gained access to the network by posing as an OPM contractor. And while Government officials have never been able to place the blame directly on a country, they believe the hacker was state sponsored by China.

Read the full article here.

U.S. JUSTICE DEPARTMENT TO END TRUMP-ERA PROGRAM TARGETING THREATS POSED BY CHINA

Sarah N. Lynch | Reuters | February 23, 2022

The U.S. Justice Department on Wednesday will end a program focused on fighting Chinese espionage and intellectual property theft, shifting from what an official called a "myopic" focus to address threats from a broader array of hostile nations. Critics have said the initiative, put in place during former President Donald Trump's administration, amounted to racial profiling and that it created a culture of fear that has chilled scientific research. The move, the details of which were reported by Reuters earlier this month, is a recognition that the focus on China was too limited, said Matt Olsen, the Assistant Attorney General for the National Security Division. "We see nations such as China, Russia, Iran and North Korea becoming more aggressive and more capable in their nefarious activity than ever before," Olsen said in a speech at George Mason University's National Security Institute. "Our new strategy is threat-driven." The department's "China Initiative," started in 2018, has faced intense scrutiny by civil rights groups and some members of Congress for its expansive investigation into professors at U.S. universities over whether they disclosed financial ties to China when seeking federal grant funding and visiting Chinese scholars from military affiliated universities.

Read the full article here.

THE CYBER SOCIAL CONTRACT

Chris Inglis and Harry Krejsa | Foreign Affairs | February 21, 2022

In the spring of 2021, a Russia-based cybercrime group launched a ransomware attack against the largest fuel pipeline in the United States. According to the cybersecurity firm Mandiant, the subsequent shutdown and gas shortage across the East Coast likely originated from a single compromised password. That an individual misstep might disrupt critical services for millions illustrates just how vulnerable the United States' digital ecosystem is in the twenty-first century. Although most participants in the cyber-ecosystem are aware of these growing risks, the responsibility for mitigating systemic hazards is poorly distributed. Cyber-professionals and policymakers are too often motivated more by a fear of risk than by an aspiration to realize cyberspace's full potential. Exacerbating this dynamic is a decades-old tendency among the large and sophisticated actors who design, construct, and operate digital systems to devolve the cost and difficulty of risk mitigation onto users who often lack the resources and expertise to address them.

Read the full article here.

WHAT IS DISTINCT ABOUT CHINA'S DEVELOPMENT OF HIGHER EDUCATION?

Miguel Antonio Lim | Asian Polyglot View | February 20, 2022

The recent spectacle of the Winter Olympics opening in Beijing was an opportunity to reflect on the change in China and its relationship with world society since the city hosted the 2008 Summer Olympics. Partly due to the pandemic, the opening ceremony appeared to be a much more restrained affair in comparison to the overtly triumphant tone of the previous ceremony, which seemed designed to stamp the country's emergence on the world stage. China's current hosting of the Olympics is subject to a variety of issues, including diplomatic protests. But it is also marked by an approach that seems more confident about the country's global role and position. This confidence and increased assertiveness are not only evident in the field of sport, but also in many other fields, including China's policies and practices in international higher education. The rapid economic and political rise of China, accentuated by events like the Olympics, contributes to the sense that China is unique – that its size and politics distinguish it from every other nation.

Read the full article here.

OPEN SOURCE CODE: THE NEXT MAJOR WAVE OF CYBERATTACKS

James Carder | Dark Reading | February 21, 2022

Open source software is ubiquitous. It has become an unequaled driver of technological innovation because organizations that use it don't have to reinvent the wheel for common software components. However, the ubiquity of open source software also presents a significant security risk, as it opens the door for vulnerabilities to be introduced (intentionally or inadvertently) to the consumers of open source software products. The recent race to address major vulnerabilities in the widely used Log4j code library is the biggest sign yet that risks within the open source software environment must be addressed. The open source attack method is appealing to bad actors because it can be widespread and highly effective. Attackers can use various methods to obfuscate malicious changes contributed to open source projects, and the rigor in reviewing code for security implications can vary widely across projects. Without stringent controls in place to detect these malicious changes, they may go unnoticed until after they've been distributed and included in software across numerous companies.

Read the full article here.

DARPA SCREENS FOR "RISK" IN RESEARCHERS' FOREIGN AFFILIATIONS

Mitch Ambrose | Physics Today | February 18, 2022

The Defense Advanced Research Projects Agency has implemented a new review process for the research projects it funds that assesses risks posed by funding applicants' affiliations with foreign institutions. The agency's new Countering Foreign Influence Program, which applies to fundamental research projects, was announced in September and revised in December. Other federal science agencies have likewise expanded their use of disclosure policies to identify problematic conflicts of interest and time commitment. DARPA's policy goes further by tying the review process to specific categories of foreign entities of concern. Although the agency stresses that projects deemed to carry high risk can still proceed with the appropriate approval, many stakeholders are seeking more clarity on the kinds of affiliations DARPA and other science agencies might deem problematic. The new policy is a product of more than three years of DOD efforts to respond to congressional direction to secure the research it funds from potential exploitation by rival governments.

Read the full article here.

UNIVERSITIES SHOULD DO MORE TO RAISE AWARENESS OF SECURITY ISSUES WITH THEIR RESEARCHERS

FE News | February 17, 2022

A new @HEPI_news report, What's next for national security and research? by Dr Alexis Brown (HEPI Report 147), reviews what measures are in place to protect UK research from foreign interference, including the new National Security and Investment Act (2021) that came into force on 4 January 2022. It argues that, while universities can do more to raise awareness of security issues with their researchers, any new legislative measures must also be carefully designed to avoid increasing administrative burdens in counterproductive ways. The National Security and Investment Act (NSIA) (2021) gives the Government new powers, based in the Department for Business, Energy and Industrial Strategy (BEIS), to intervene in the acquisition of UK entities and assets by both foreign and domestic investors. The NSIA's scope goes significantly beyond its global equivalents, according to experts. As Michael Leiter, former Director of the United States National Counterterrorism Center, noted in testimony to the House of Commons, the UK will see an 'explosive increase in matters' under this new regime, as it goes from reviewing very few cases to over a thousand each year.

Read the full article here.

OVERSEAS CHINESE STUDENTS AND SCHOLARS IN CHINA'S DRIVE FOR INNOVATION

Anastasya Lloyd-Damnjanovic and Alexander Bowe | U.S.-China Economic and Security Review Commission | October 7, 2020

This report surveys an array of programs and policies the Chinese government has established over decades to exploit the scientific expertise of Chinese students and scholars studying in the United States for the purpose of accelerating China's economic and military modernization. While the report examines the elaborate system of incentives the Chinese government employs to induce Chinese students and scholars to contribute scientific expertise to China's national modernization goals, it does not intend to "profile" students from China, or to evaluate the degree of agency Chinese students and scholars have when faced with the opportunity to participate in these government-sponsored programs. This report assumes these programs target a minority of the overall Chinese student body, and that the majority of Chinese students contribute positively to U.S. research and society. Chinese leaders have long viewed advanced science and technology (S&T) as key to China's comprehensive national power and sought to acquire it through licit and illicit means from developed countries like the United States. Since the 1990s, China's government has built a sprawling ecosystem of structures, programs, and incentives to coopt and exploit Chinese students and scholars for the S&T they acquire abroad.

Read the full article here.