ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

March 15, 2023

U.S. LAUNCHES 'DISRUPTIVE TECHNOLOGY' STRIKE FORCE TO TARGET NATIONAL SECURITY THREATS

James Pearson and Sarah N. Lynch | Reuters | February 16, 2023

A top U.S. law enforcement official on Thursday unveiled a new "disruptive technology strike force" tasked with safeguarding American technology from foreign adversaries and other national security threats. Deputy Attorney General Lisa Monaco, the No. 2 U.S. Justice Department official, made the announcement at a speech in London at Chatham House. The initiative, Monaco said, will be a joint effort between her department and the U.S. Commerce Department, with a goal of blocking adversaries from "trying to siphon our best technology." Monaco also addressed concerns about Chinese-owned video sharing app TikTok. The U.S. government's Committee on Foreign Investment in the United States (CFIUS), a powerful national security body, in 2020 ordered Chinese company ByteDance to divest TikTok because of fears that user data could be passed on to China's government. The divestment has not taken place. CFIUS and TikTok have been in talks for more than two years aiming to reach a national security agreement. "I will note I don't use TikTok, and I would not advise anybody to do so because of these concerns.

Read the full article here.

PENTAGON BOOSTS SPENDING ON R&D, JADC2 AND CYBERSECURITY IN $145B BUDGET

Jaspreet Gill | Breaking Defense | March 13, 2023

The Pentagon today released its largest research, development, test and evaluation (RDT&E) budget request at $145 billion, including funding for major initiatives like Joint All Domain Command and Control (JADC2), rapid experimentation and advanced technology areas as it sharpens its focus on modernization to stay ahead of foreign adversaries. DoD's RDT&E budget request has been on an uptick over the past few years: In fiscal 2023, the department requested $130.1 billion in funding, a 9.5 percent increase over FY22. The FY24 request represents another 4 percent increase from FY23 levels, according to budget documents. Although the Pentagon has not yet disclosed how much of the RDT&E funding will go into which specific programs, the department did reveal that it's requesting some $17.8 billion for "science and technology efforts" with $9.3 billion of that going to advanced technology and $2.5 billion for basic research. It also highlighted a few key individual initiatives. For one key effort aimed at addressing capability gaps and emerging technologies, the Rapid Defense Experiment Reserve (RDER), the department is asking for $687 million, almost double what it requested in FY23.

Read the full article here.

COUNTERING CHINA REQUIRES A NEW APPROACH TO COUNTERINTELLIGENCE

Greg Levesque | The Well News | March 9, 2023

The Chinese balloon moving over the continental United States last month, as we know now, was not some rogue surveillance operation gone wrong. Instead, it was part of a broader surveillance program that China directed over the past few years. This should come as no surprise. China and its leaders are clear about what their national priorities are, and once determined, the country uses all aspects of its military and civilian infrastructure to achieve its goals. That's the case with this surveillance program, and it's also the case with the long-standing effort to steal the intellectual property of U.S.-based companies, particularly in strategic areas including quantum computing, AI, autonomous vehicles, drones or even rare-earth metals and semiconductors. The cost of China's activities against U.S. businesses alone has been pegged at $600 billion a year. The United States finds itself in a multi-front battle with China for both geopolitical and technological dominance.

Read the full article here.

CANADA MOVES TO BAN FUNDING FOR 'RISKY' FOREIGN COLLABORATIONS

Jeffrey Mervis | Science | February 17, 2023

Canada's three major national research agencies will no longer fund proposals from scientists doing "sensitive research" that involves foreign collaborators deemed to pose a security risk to the country. Although the new policy, announced on 14 February, doesn't mention China, it parallels actions taken in recent years by the United States, Australia, and other countries to prevent their research investments from benefiting China's ruling party or military. Under the new rules, defense and intelligence officers will do a second vetting of proposals that scientists have already flagged as potentially problematic. But some Canadian researchers fear the additional security review could eliminate collaborations with China that now benefit Canada. They also want the government to spell out how it will decide which proposals pose too great a risk. "Are we moving to a situation in which the intelligence community will be dictating what research will be funded?" asks Tamer Özsu, a computer scientist at the University of Waterloo.

Read the full article here.

NORTH KOREAN HACKERS USED POLISHED LINKEDIN PROFILES TO TARGET SECURITY RESEARCHERS

AJ Vicens | CyberScoop | March 10, 2023

Hackers believed to be working on behalf of North Korea have in recent years posed as recruiters and targeted workers in a variety of industries with offers of extravagant jobs at big-name firms with massive salaries. In the past, that campaign has mostly been carried out over email, but now researchers are seeing North Korean hackers shift their phishing attempts to LinkedIn and WhatsApp. By first constructing convincing profiles on the career-focused social media platform LinkedIn, reaching out to their victims with phony job offers and convincing them to move the conversation over to WhatsApp, where they would be targeted with malware, North Korean hackers have crafted a sophisticated method for targeting computer security researchers, according to a two-part report released by Google's Mandiant on Thursday. Michael Barnhart, a principal analyst at Mandiant, describes this North Korean threat actor as "one of the more skilled groups coming out of this closed off nation," and in targeting security researchers, the group deployed a range of new tools.

Read the full article here.

NSA RELEASES RECOMMENDATIONS FOR MATURING IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT IN ZERO TRUST

National Security Agency | March 14, 2023

The National Security Agency (NSA) released the "Advancing Zero Trust Maturity throughout the User Pillar" Cybersecurity Information Sheet (CSI) today to help system operators' mature identity, credential, and access management (ICAM) capabilities to effectively mitigate certain cyber threat techniques. Cybersecurity incidents are on the rise due to immature capabilities in identity, credential, and access management (ICAM) of national security, critical infrastructure, and Defense Industrial Base (DIB) systems. The Zero Trust model limits access to only what is needed and assumes that a breach is inevitable or already occurred. Adoption of a Zero Trust cybersecurity framework is part of the National Cybersecurity Strategy and is directed by the President's Executive Order on Improving the Nation's Cybersecurity (EO 14028) and National Security Memorandum 8 (NSM-8), for Federal Civilian Executive Branch (FCEB) agencies and National Security System (NSS) owners and operators.

Read the full article here.

COLLABORATIVE ADVANTAGE: CREATING GLOBAL COMMONS FOR SCIENCE, TECHNOLOGY, AND INNOVATION

Leonard Lynn and Hal Salzman | Issues in Science and Technology | March 6, 2023

What was once described as the "American Century" of political and technological dominance is giving way to a polycentric world. In this new order, the fate of nations will depend on international collaboration for innovation and prosperity, particularly as global challenges including disease, poverty, energy deficits, and climate change threaten all. The innovations needed can no longer be produced by only a few nations, nor can the benefits be confined to those few. Developing such innovations, however, will require collaborative efforts at a global scale that go beyond anything previously attempted. In the postwar decades, the United States pursued a techno-nationalist path in research and development that became a global norm. The US government was capable of funding research projects at far higher levels than other governments; US firms also directed substantial portions of revenue to R&D, extending federal efforts. The world's most advanced R&D laboratories included the largely independent Bell Labs and Xerox PARC, while companies like IBM, GE, RCA, DuPont, and Polaroid were engaged in significant basic and exploratory research.

Read the full article here.

REQUEST FOR INFORMATION; NSPM 33 RESEARCH SECURITY PROGRAMS STANDARD REQUIREMENT

Federal Register | Office of Science and Technology Policy | March 7, 2023

The Office of Science and Technology Policy (OSTP) requests comments from the public on draft Research Security Programs Standard Requirement developed in response to National Security Presidential Memorandum 33 on National Security Strategy for United States Government-Supported Research and Development (R&D). The draft Standard Requirement has been created by OSTP, together with Federal agencies and the Office of Management and Budget, to ensure that there is uniformity across Federal research agencies in implementing this requirement. Interested persons and organizations are invited to submit comments on or before 5 p.m. ET June 5, 2023. Submit comments electronically to *researchsecurity@ostp.eop.gov* with the subject line *Comment on Research Security Programs* by the deadline. Due to time constraints, mailed paper submissions will not be accepted. Response to this notice is voluntary.

Read the full article here.

NIST PLOTS BIGGEST EVER REFORM OF CYBERSECURITY FRAMEWORK

Emma Woollacott | The Daily Swig | February 23, 2023

The US National Institute of Standards and Technology (NIST) is planning significant changes to its Cybersecurity Framework (CSF) – the first in five years, and the biggest reform yet. First published in 2014 and updated to version 1.1 in 2018, the CSF provides a set of guidelines and best practices for managing cybersecurity risks. The framework is designed to be flexible and adaptable rather than prescriptive, and is widely used by organizations and government agencies, both within and outside the US, to create cybersecurity programs and measure their maturity. Following a long consultation, NIST has published a concept paper (pdf) for CSF 2.0 and opened it up to further review. The resulting feedback will be used to develop a final draft of the revised framework, due out sometime this summer. "We think that there's been enough changes in the cybersecurity landscape to warrant a significant update this time around," says Cherilyn Pascoe, senior technology policy advisor at NIST and Cybersecurity Framework Program lead.

Read the full article here.

CHINA USING LINKEDIN, INDEED TO RECRUIT SPIES, TARGET EXPERTS IN US

Kellie Meyer and Zoe Lake | NewsNation | March 6, 2023

Job portals like LinkedIn and Indeed are popular among job-seekers and recruiters alike, but national security experts warn the platforms have become hunting grounds for foreign spies. "They're going after every sector in the U.S. economy," said Mirriam-Grace MacIntyre, executive director of the National Counterintelligence and Security Center. "They're looking for people who are in academia, who are in research and development, who are in the private sector.". Have Chinese spies infiltrated US college campuses? The sheer scale of the espionage effort has been amplified by social media, which allows agents from countries like China to engage with tens of thousands of people online without ever meeting them. "(Foreign adversaries) only need 1% to say yes," said Alan Kohler, assistant director of the FBI's Counterintelligence Division. "That's the problem that we face on the counterintelligence side." Kohler's job is to help protect America's secrets, but sites like LinkedIn and Indeed have brought on new challenges for him and his team.

Read the full article here.

SAFEGUARDING RESEARCH AT ONTARIO'S UNIVERSITIES

Ontario's Universities | Council of Ontario Universities | February 2023

While openness, collaboration, equity, diversity and inclusion are critical to discovery and innovation, Ontario's universities recognize that vigilance is critical to preventing loss of opportunities, as well as to ensuring research conducted on campuses continues to be converted into tangible benefits and economic prosperity. With a shared goal to safeguard Canada's research ecosystem, Ontario's universities are partnering with all levels of government – as well as allies through the G7 research security and integrity working group – to ensure research is secure. In today's rapidly shifting geo-political environment, research security will continue to be a priority for universities across the province, as university research offices continue to take reasonable and risk-based measures to safeguard investments in research. In fact, many Ontario universities have been leaders in establishing a national security framework for university research and have driven the creation of the Government-Universities Working Group on Research Security.

Read the full article here.

SAFEGUARDING OUR FUTURE – PROTECTING PERSONAL HEALTH DATA FROM FOREIGN EXPLOITATION

The National Counterintelligence and Security Center | January 31, 2022

Foreign companies and some U.S. businesses with facilities abroad have been partnering or contracting with U.S. organizations to provide diagnostic tests and services that in some cases collect specimens, DNA, fitness / lifestyle information, or other personal health data from patients or consumers in the United States. Some of these companies may be subject to foreign laws that can compel them to share such data with foreign governments, including governments that exploit personal health data for their own ends and without regard to individual privacy. For example, several Chinese companies have partnered or contracted with U.S. organizations and are accredited, certified, or licensed to perform genetic testing or whole-genome sequencing on patients in the U.S. healthcare system, potentially giving them direct access to the genetic data of patients in the United States.[1] Chinese companies are compelled to share data with the government of the People's Republic of China,[2] which has used genetic data for state surveillance and repression of its ethnic and religious minorities,[3],[4] as well as for military research and applications.[5]

Read the full article here.

COUNTERING FOREIGN INTERFERENCE

Government of Canada | Public Safety Canada | March 10, 2023

As an advanced economy and open democracy, Canada is a target of foreign interference. Foreign interference includes harmful activities undertaken by foreign states, or those acting on its behalf, that are clandestine, deceptive, or involve a threat to any person to advance the strategic objectives of those states to the detriment of Canada's national interests. Foreign interference poses one of the greatest strategic threats to Canada's national security. Examples include: Threats, harassment or intimidation by foreign states, or those acting on its behalf, against anyone in Canada, Canadian communities, or their loved ones abroad; and, Targeting officials at all levels of government to influence public policy and decision-making in a way that is clandestine, deceptive or threatening. The Government of Canada has a number of resources to ensure that the public has the necessary knowledge and tools to be able to recognize foreign interference when encountered.

Read the full article here.

CHINA'S SECURITIZATION OF GENETIC RESEARCH

Patrick Beyrer | The Diplomat | March 13, 2023

Since the beginning of the pandemic, international scientific research cooperation with China has plummeted. Between navigating border closures, obstacles to equipment access, and increasingly tense domestic political climates, researchers worldwide have encountered a "chilling effect" in life sciences research and development when it comes to working with China. Scientists in the United States are reluctant to start new or continuing existing collaborations with their Chinese peers. But the largest block to Sino-global public health collaboration is China's own legislative push against it. Since 2015, China has initiated a series of reforms in biotechnology that has securitized the industry to an extreme. The National Security Law that year reserved China's right to "improve the handling of public health, public safety, and other types of outbreaks that affect national security and social stability," linking biosafety to national security. In 2016, the State Council's "Guiding Opinions on the Application and Development of Big Data in Healthcare" labeled biomedical data an "important, foundational strategic state resource." The same year, amendments to human genetic resource (HGR) governance introduced "safeguarding national security" as a core government mandate in the field.

Read the full article here.

CHINA DIVERTS SOME RESEARCHERS TO CANADA AFTER U.S. VISA DENIALS, CSIS SAYS

National Post Today | March 13, 2023

Beijing is using a "workaround strategy" for postgraduate researchers to study cutting-edge technology at Canadian and U.S. universities after Washington began denying visas for some Chinese students on the grounds that they might steal intellectual property with military uses, according to a Canadian Security Intelligence Service report. The Dec. 21, 2021, report, labelled secret and viewed by The Globe and Mail, said the strategy sends some scholarship students to Canada from the People's Republic of China (PRC) with the aim of gaining access to critical high tech. The Chinese government's game plan includes training these Chinese citizens on how to avoid drawing too much attention when studying abroad. The CSIS report lays out how China is using students to obtain technology that could be of benefit to the Chinese military, such as quantum computing, big data and artificial intelligence. The report was shared across key government departments and with the CIA, FBI and Britain's domestic intelligence service, M15, as well as Australian and New Zealand authorities.

Read the full article here.