RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE

THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

September 26, 2024

JUSTICE DEPARTMENT ANNOUNCES FIVE CASES TIED TO DISRUPTIVE TECHNOLOGY STRIKE FORCE

U.S. Department of Justice | Press Release | September 16, 2024

The Justice Department today announced criminal charges in five cases from four U.S. Attorney's offices in connection with the multi-agency Disruptive Technology Strike Force (Strike Force). The Strike Force is co-led by the Departments of Justice and Commerce to counter efforts by hostile nation states to illicitly acquire sensitive U.S. technology to advance their authoritarian regimes and facilitate human rights abuses. Launched in February 2023, the Strike Force's work has led to the unsealing of charges against 34 defendants in 24 cases involving alleged export control violations, smuggling, theft of trade secrets, and other charges by actors connected to Russia, China, and Iran. The cases announced today took place over the course of multiple weeks, culminating in the arrest today of a Russian national allegedly seeking to illegally export electronics for use in Unmanned Aerial Vehicles (UAVs) to Russia. The other cases also cover spearfishing of U.S-based scientists by an employee of a state-owned Chinese defense company and the smuggling of laser welding machines used in nuclear munition production to Russia.

Read the full article here.

BIS IMPOSES $5.8 MILLION PENALTY AGAINST PENNSYLVANIA COMPANY FOR SHIPMENTS OF LOW-LEVEL ITEMS TO PARTIES TIED TO THE PRC'S HYPERSONICS, UAV, AND MILITARY ELECTRONICS PROGRAMS

Bureau of Industry & Security | Press Release | August 15, 2024

Today, as part of a settlement agreement to resolve alleged violations of U.S. export controls, the Department of Commerce's Bureau of Industry and Security (BIS) imposed a $5.8 million civil penalty against TE Connectivity Corporation (TE), located in Middletown, Pennsylvania, and TE Connectivity HK Limited, located in Kwai Chung, New Territories, Hong Kong, for shipments of low-level items to parties tied to the People's Republic of China's (PRC) hypersonics, unmanned aerial vehicles (UAV), and military electronics programs. "When we announced the Disruptive Technology Strike Force with the Department of Justice last year, we made clear that all tools, including BIS's unique administrative enforcement capabilities, would be leveraged to punish those who send even low-level technology to nation-state adversaries if that technology has the potential to further the development of unmanned aerial vehicle and hypersonic weapons programs," said Assistant Secretary for Export Enforcement Matthew S. Axelrod.

Read the full article here.

CAUTIOUS OPTIMISM ON OSTP RESEARCH CYBERSECURITY REQUIREMENTS

Jarret Cummings | EDUCAUSE | September 11, 2024

In early 2023, the White House Office of Science and Technology Policy (OSTP) released its initial proposal for a "research security program standard requirement." All federal research funding agencies would have to apply the requirement to colleges and universities that receive more than $50 million per year in federal research funding.Footnote1 The development of these comprehensive research security mandates stems from National Security Presidential Memorandum – 33 (NSPM-33), "Supported Research and Development National Security Policy." When finalized, the "standard requirement" would establish the basic parameters for the research security programs that covered institutions must have in place to continue competing for federal research grants. Most of the proposed framework addresses research security issues such as faculty conflicts of interest and commitment and research talent recruitment programs of foreign governments. However, it also includes a research cybersecurity section that essentially would make the cybersecurity guidelines for Federal contract information (FCI) the standards for higher education research cybersecurity.

Read the full article here.

HOW NIH RESPONDS TO ALLEGATIONS OF FOREIGN INTERFERENCE

National Institute of Allergy and Infectious Diseases | September 10, 2024

Most NIH grant awards go to domestic organizations, but we welcome applications from foreign organizations that include talent, resources, populations, or other resources not found in the United States. Even for domestic grant recipients, establishing partnerships with foreign researchers can be critical for access to a unique study population or an emerging infectious disease (we refer to these as "foreign components"). Academic research activities—writing a letter of recommendation for a foreign scientist, coauthoring scientific publications, or lecturing or teaching abroad—are commonplace. At the same time, NIH maintains Requirements for Disclosure of Other Support, Foreign Components, and Conflicts of Interest. NIH staff use that information to help ensure funded projects do not receive duplicative support, research is conducted objectively, and sensitive data are kept confidential. The disclosure requirements align with National Security Presidential Memorandum (NSPM-33)—Supported Research and Development National Security Policy.

Read the full article here.

THE NEW NORMS OF RESEARCH: COMPLIANCE WITH FUNDER AND GOVERNMENT POLICIES

Highwire | September 10, 2024

In a landscape continually reshaped by evolving policies and mandates, understanding the intricacies of research funding, open access, and compliance becomes crucial for researchers, publishers, and academic institutions alike. This blog is based on HighWire Press's Best Practices webinar, Complying with Funder and Government Mandates. It was a discussion among industry leaders Shauna Sadler from ORCID, Sharon Jackson and John McCrow from Jisc on the current state and future directions of research funding, highlighting the critical role of government and private foundations in shaping the trajectory of scholarly work. With a focus on the strings attached to research funding – from data deposit requirements to open access mandates – the webinar offered a comprehensive overview of the challenges and opportunities in the academic research landscape.

Read the full article here.

DEAR COLLEAGUE LETTER: REQUEST FOR INFORMATION ON THE CHIPS AND SCIENCE ACT SECTION 10343. RESEARCH ETHICS

U.S. National Science Foundation | September 9, 2024

The U.S. National Science Foundation (NSF) is an independent federal agency that supports research at the frontiers of current knowledge, across all fields of science, engineering and education in all 50 states and U.S. territories. NSF is issuing this Request for Information (RFI) to seek input to inform the development of the agency's response to Section 10343. Research Ethics in the CHIPS and Science Act of 2022 (Public Law 117-167). NSF welcomes feedback from interested parties. This includes representatives from non-profit organizations, philanthropies, industry, local, state, and tribal government offices/agencies, K-12 schools and districts, institutions of higher education, trade, and/or vocational schools. While the NSF has funding opportunities in the area of ethical and societal risks such as Ethical and Responsible Research (ER2) and Responsible Design, Development, and Deployment of Technologies (ReDDDoT), this Dear Colleague Letter (DCL) does not itself invite research proposals nor is it a funding opportunity. However, the submission of collective input to this RFI spanning different perspectives from multiple constituent communities may be used to inform, refine, and catalyze future NSF investments, policies, and programs.

Read the full article here.

CHINA WORKS WITH ITS CYBERSECURITY RESEARCHERS—CAN THE US DO THE SAME?

Eoin Higgins | IT BREW | September 17, 2024

Should the US government follow China's lead and be more proactive in how it works with hackers? Kara Sprague, incoming CEO of HackerOne, argues that there are some aspects of the Chinese system the West could emulate. "I have not seen North America or even the United States organize that level of defense activity, so to speak, or try to proactively identify those vulnerabilities and fix them," Sprague told IT Brew. "And so I think there is something to be learned from how different nations are addressing these issues." Locked down. There are some government-sponsored hacking contests in the US. Hack the Pentagon, a competition to break through Department of Defense protections, has been running since 2016. In 2023, the White House launched an AI-based hacking challenge with the Defense Advanced Research Projects Agency, commonly known by its acronym, DARPA.

Read the full article here.

HOUSE PUSHES TO RESURRECT CHINA INITIATIVE

Lindsay McKenzie | American Institute of Physics (AIP) | September 18, 2024

The House approved legislation last week that would reinstate the Department of Justice's controversial China Initiative over the objections of critics who argue it was biased against Asian American academics. The bill passed on a vote of 237-180, with support from 214 Republicans and 23 Democrats. The Protect America's Innovation and Economic Security from CCP Act would require the DOJ to launch a "CCP Initiative" that aims to "curb spying by the Chinese Communist Party on United States intellectual property and academic institutions," among other goals. The legislation is unlikely to advance in the Democrat-controlled Senate, where the companion bill has only Republican cosponsors. In addition, the White House issued a statement strongly opposing the bill last week, stating it "could give rise to incorrect and harmful public perceptions that DOJ applies a different standard to investigate and prosecute criminal conduct related to the Chinese people or to American citizens of Chinese descent."

Read the full article here.

CONGRESS TARGETS CHINESE INFLUENCE IN HEALTH TECH. IT COULD COME WITH TRADEOFFS

Didi Tang and Haven Daley | The Associated Press | September 13, 2024

A California biotechnology company that helps doctors detect genetic causes for cancer is among those that could be cut out of the U.S. market over ties to China, underscoring the possible tradeoffs between health innovation and a largely bipartisan push in Congress to counter Beijing's global influence. The competition between the world's superpowers is hitting Complete Genomics, whose employees, some in white lab coats stitched with U.S. flag arm patches, spin samples in test tubes and huddle around computers in San Jose. Its founder and chief scientific officer said he's frustrated that geopolitics is interfering with science. "It's just a loss for the research and for the industry," Radoje Drmanac said. The U.S. House this week overwhelmingly passed the BIOSECURE Act, which cites national security in preventing federal money from benefiting Complete Genomics and four other companies linked to China. They work with U.S. drugmakers to develop new medications or help doctors diagnose diseases. It is part of a sweeping package of bills aimed at countering China's influence and power, especially in technology, that Congress largely backed this week.

Read the full article here.

CHINA'S UNIQUE PATH TO SCIENTIFIC AND TECHNOLOGICAL POWER

Caroline S. Wagner | University World News | September 18, 2024

China's stunning rise to world-class levels in science and technology defied most predictions. In 1980, China was barely a blip on the scientific radar. In a magnanimous gesture by Western diplomats, agreements were signed to encourage cooperation in science and technology. The signatures were inked in the spirit of goodwill, and with the implicit belief that, with prosperity, China would in turn adopt liberal and democratic governance. China certainly mastered these lessons in science and technology. In 1990, Chinese authors produced less than 2% of articles in Web of Science. In 2023, they dominate with 25% of all articles – the largest contributing nation to the Web of Science (the United States has held the top spot since 1948 when it grabbed the lead from the United Kingdom).

Read the full article here.

CHINA IS RAPIDLY BECOMING A LEADING INNOVATOR IN ADVANCED INDUSTRIES

Robert D. Atkinson | Information Technology & Innovation Foundation (ITIF) | September 16, 2024

Perhaps the most critical question for the United States vis-à-vis China's economic and technology challenge is whether China can become a real innovator. If China has difficulty becoming an innovator and remains largely a copier, then the threat to the United States and other allied technology economies is less. In this case, as long as the United States (and allies) can innovate at a robust-enough rate, they can likely maintain the lead on advanced technologies, even if China quickly copies foreign innovations. But if China can develop new-to-the-world innovations ahead of, or at the nearly the same time as, the United States and allied nations, its potential to displace U.S. (and allied) technology-based companies and capabilities becomes much more likely, especially because China benefits from significant economies of scale and a government laser focused on global best-in-class science and technology policy for competitiveness.

Read the full article here.

FINAL U.S. MISCONDUCT RULE DROPS CONTROVERSIAL CHANGES

Jeffrey Mervis | Science | September 13, 2024

The U.S. agency that investigates research misconduct by federally funded biomedical scientists has dropped a controversial proposal that would have allowed it to publicize previously undisclosed misconduct findings by universities. In announcing the first revision of its research misconduct policy in 20 years, the federal Office of Research Integrity (ORI) said it removed the draft provision in response to complaints from many institutions about "regulatory overreach" and possible "breaches of confidentiality." ORI also:

- dropped a proposed 30-day deadline for starting an inquiry after an institution first receives an allegation of possible misconduct;
- restored a university's ability to forgo a full investigation if it decides the conduct was the result of "honest error"; and
- withdrew a requirement that institutions record and transcribe all statements obtained during an initial review of the allegations.

Read the full article here.

TIKTOK SAYS IT'S NOT SPREADING CHINESE PROPAGANDA. THE U.S. SAYS THERE'S A REAL RISK. WHAT'S THE TRUTH?

Ken Dilanian | NBC News | September 16, 2024

Is TikTok trying to secretly influence Americans at the behest of the Chinese government? That question is at the heart of the legal battle over a law passed by Congress that could result in a ban on the popular social media company in the United States — a clash that will play out in court Monday as each side presents oral arguments in a Washington, D.C., courtroom. In court documents filed in advance of the hearing — heavily redacted, because they contain classified information — the Justice Department and a senior U.S. intelligence official say flatly that they have no direct evidence China has used TikTok for propaganda purposes in the U.S. They also say there is significant risk that could happen. But a pair of academic studies — cited in the court documents and congressional testimony — make the case that the platform is biased in favor of Chinese government views, including suppressing information on China's treatment of its Uyghur minority and its actions in Tibet.

Read the full article here.

U.S. RESEARCH AIDED CHINESE MILITARY TECHNOLOGY, HOUSE REPUBLICANS SAYE

Ana Swanson | The New York Times | September 23, 2024

A House committee focused on threats from China argues in a new report that U.S. federal research funding had helped to advance Chinese technologies with military applications, fueling a potential national security rival to the United States. The report argues that Chinese partnerships with U.S.-funded researchers and universities have helped to propel Beijing's advancements in fields like hypersonic and nuclear weapons, artificial intelligence and semiconductors, and that these developments may one day influence how the two nations perform on the battlefield. The report — put out by the Republican members of the House Select Committee on the Chinese Communist Party and the House Committee on Education and the Workforce — also recommends stricter guidelines around federally funded research, including significantly curtailing the ability of researchers who receive U.S. grants to work with Chinese universities and companies that have military ties.

Read the full article here.

HOW AMERICAN TAXPAYERS AND UNIVERSITIES FUND THE CCP'S ADVANCED MILITARY AND TECHNOLOGICAL RESEARCH

United States Congress | Majority Staff Report | September 2024

The Chinese Communist Party (CCP) exploits federally funded research and partnerships between U.S. universities and People's Republic of China (PRC) defense-linked universities to achieve technological breakthroughs, both in technologies with military applications and in critical and emerging technologies where the PRC lags behind the U.S. and its allies. Our investigation found that due to a lack of legal guardrails around federally funded research, hundreds of millions of dollars in U.S. federal research funding over the last decade have contributed to the PRC's strategic goals by helping the PRC achieve advancements in dual use, critical, and emerging technologies like hypersonic weapons, artificial intelligence, fourth generation nuclear weapons technology, and semiconductor technology. Specifically, we examined research publications that disclose funding from the Department of Defense (DOD) or the U.S. intelligence community (IC) and include a collaboration between a federally funded researcher(s) and a researcher(s) affiliated with PRC institutions, most frequently PRC universities.

Read the full article here.

NSA AND ALLIES ISSUE ADVISORY ABOUT PRC-LINKED ACTORS AND BOTNET OPERATIONS

National Security Agency/Central Security Service | Press Release | September 18, 2024

The National Security Agency (NSA) joins the Federal Bureau of Investigation (FBI), the United States Cyber Command's Cyber National Mission Force (CNMF), and international allies in releasing new information about People's Republic of China (PRC)-linked cyber actors who have compromised internet-connected devices worldwide to create a botnet and conduct malicious activity. The Cybersecurity Advisory (CSA) released by the agencies, "People's Republic of China-Linked Actors Compromise Routers and IoT Devices for Botnet Operations," highlights the threat posed by these actors and their botnet, a network of compromised nodes positioned for malicious activity. "The botnet incorporates thousands of U.S. devices with victims in a range of sectors," said Dave Luber, NSA Cybersecurity Director. "The advisory provides new and timely insight into the botnet infrastructure, the countries where compromised devices are located, and mitigations for securing devices and eliminating this threat."

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

USEFUL RESOURCES

BEYOND AWARENESS TRAINING: TRANSFORMING HUMAN RISK MANAGEMENT INTO A STRATEGIC ADVANTAGE

Chris Madeksho | EDUCAUSE | September 3, 2024

In today's digital landscape, where data breaches and cyber threats are everywhere, organizations must recognize that human behavior represents a critical vulnerability. According to the 2024 Verizon Data Breach Investigations Report, nearly seventy percent of data breaches involve human interaction.[1] This statistic underscores a pressing need to shift how organizations approach cybersecurity beyond traditional technical measures.

View the full resource here.

BUILDING A CYBERSECURITY AND PRIVACY LEARNING PROGRAM: NIST PUBLISHES SP 800-50R1

National Institute of Standards and Technology | September 12, 2024

NIST Special Publication (SP) 800-50r1 (Revision 1), Building a Cybersecurity and Privacy Learning Program, provides updated guidance for developing and managing a robust cybersecurity and privacy learning program in the Federal Government. This revision was informed by National Defense Authorization Act (NDAA) for FY2021, the Cybersecurity Enhancement Act of 2014, and the NICE Workforce Framework for Cybersecurity (NICE Framework). In addition, the 2016 update to Office of Management and Budget (OMB) Circular A-130 emphasizes the role of both privacy and security in the federal information life cycle and requires agencies to have both security and privacy awareness and training programs.

View the full resource here.

INTERNATIONAL TALENT PROGRAMS IN THE CHANGING GLOBAL ENVIRONMENT: PUBLIC RELEASE LAUNCH

Jordan Graves | National Academies | August 29, 2024

The public release of the International Talent Programs in the Changing Global Environment consensus study report was held on August 29, 2024, 3:00-4:00 PM ET. The report reviews foreign and domestic talent or incentive programs and recommends ways to improve the effectiveness of U.S. mechanisms for attracting and retaining the best and brightest scholars, relative to programs and incentives used by the U.S.'s strategic competitors. Members of the consensus study committee provided an overview of the report and discuss its findings and recommendations. This was followed by a moderated question and answer period during which members of the public submitted written questions. The event was recorded and the video will be posted on this page.

View the full resource here.

WHAT IS AN INFORMATION SECURITY POLICY?

Abi Tyas Tunggal | UpGuard | September 16, 2024

An information security policy (ISP) is a set of rules, policies and procedures designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements. ISPs should address all data, programs, systems, facilities, infrastructure, authorized users, third parties and fourth parties of an organization.

View the full resource here.

RESEARCH SECURITY AND INTERNATIONAL ENGAGEMENT — THOMAS MASON | 2024 HERTZ SUMMER WORKSHOP

Hertz Summer Workshop and Topical Forum | YouTube | August, 2024

At the 2024 Hertz Summer Workshop and Topical Forum, taking place August 1–4, 2024, at the Mont-Tremblant Resort in Quebec, Canada, Thomas Mason, Director of Los Alamos National Laboratory, presented, "Research Security and International Engagement from the Perspective of a National Security Laboratory." The annual Hertz Summer Workshop is the signature event for the Hertz community and one-of-a-kind gathering of some of the top scientists, entrepreneurs and leaders in our nation's science and technology enterprise.

View the full resource here.

RESEARCH SECURITY AND THE IMPACT OF AL: ADDRESSING CHALLENGES TO SAFEGUARDING, ETHICS AND COMPLIANCE

Times Higher Education Webinar | YouTube | September 18, 2024

As technology continues to shape research practices, safeguarding research has become increasingly complex. Universities face many emerging challenges, including data security, regulatory changes and concerns around the use of AI. However, technological solutions are also evolving, empowering institutions to address these issues proactively. Times Higher Education hosted a webinar on the topic – in partnership with Digital Science – to explore how institutions can confront the growing challenges in research security in an AI-driven era.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute