ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

January 26, 2023

U.S. SCIENCE BUDGETS FOR 2023 FALL SHORT OF CHIPS ACT AMBITIONS

Mitch Ambrose | American Physical Society | January 12, 2023

In the final days of 2022, and after a monthslong stalemate, Congress passed legislation that will raise the budgets of federal agencies for the rest of fiscal year 2023. Most science agencies will receive increases that keep pace with inflation; a few will see double-digit percentage boosts. However, these increases fall short of the ambitious targets Congress set in mid-2022 through the CHIPS and Science Act, which recommended ramping up budgets for three agencies — the National Science Foundation (NSF), the Department of Energy's (DOE) Office of Science, and the National Institute of Standards and Technology (NIST). The Act did have some influence: Congress gave the NSF $1 billion extra via a special supplemental appropriation. In absolute terms, it is the largest increase the agency has ever received. The supplement also includes nearly a half-billion dollars to launch a set of regional hubs for technology development that the Act authorized. The supplement increases the NSF's total budget by 12%, to $9.9 billion, for this fiscal year. But the CHIPS and Science Act recommended a 35% increase, with the aim of more than doubling the agency's budget over five years.

Read the full article here.

NIST WORKING ON 'POTENTIAL SIGNIFICANT UPDATES' TO CYBERSECURITY FRAMEWORK

Billy Mitchell | FedScoop | January 20, 2023

The National Institutes of Standards and Technology intends to release version 2.0 of its Cybersecurity Framework in the coming years, and this week, the agency teased some of the "potential significant updates" that may land in that new framework. On Thursday, NIST published a concept paper outlining significant changes to the Cybersecurity Framework and opening them to public feedback over the next several weeks. The framework is a voluntary guide to help organizations in all sectors to better understand, manage, reduce, and communicate cybersecurity risks. It is used widely, along with NIST's Risk Management Framework, by federal agencies to plan their own cybersecurity approaches. Of the proposed changes in the concept paper, the most notable are broadening the scope of the framework beyond critical infrastructure use cases to better include other organizations like small businesses and higher education institutions; including more guidance for implementation; and emphasizing the importance of cybersecurity governance and cybersecurity supply chain risk management, among others.

Read the full article here.

AGENCIES ARE ON THE HOOK TO INCREASE 'OPERATIONS SECURITY' TRAINING, EDUCATION

Justin Doubleday | Federal News Network | January 16, 2023

Agencies across government face new requirements to develop "operations security" programs to help reduce the risk of employees inadvertently exposing sensitive but unclassified information. "OPSEC" activities have traditionally been linked with military and intelligence agencies. But in a national security presidential memorandum signed in January 2021, outgoing President Donald Trump directed all executive branch departments and agencies to implement OPSEC programs, according to Rebecca Morgan, deputy assistant director for insider threat the National Counterintelligence and Security Center. "We know that adversaries, whether that's foreign intelligence entities or criminal enterprises, are targeting U.S. government information," Morgan said in an interview. "And they don't always go after the classified." The NCSC defines OPSEC as the "systematic and proven security discipline for denying adversaries the ability to collect, analyze, and exploit information, including capabilities and intentions." Examples of unclassified information officials are concerned about, Morgan said, include pre-decisional regulatory decisions that could allow someone to manipulate markets.

Read the full article here.

LIMITS AND PITFALLS OF ACADEMIC COOPERATION WITH THE PEOPLE'S REPUBLIC OF CHINA

Tobiáš Lipold | Sinopsis | January 2023

International cooperation is an important part of academic work and contributes greatly to the advancement of scientific research. In the current global trend towards a rebipolarized world, however, in which open societies are under threat from authoritarian regimes, academic contacts are becoming an instrument that some non-democratic states are using to undermine our open societies. The risks and pitfalls of academic cooperation with non-democratic states must be considered. In the case of the People's Republic of China (PRC), academic cooperation is based on a different concept of science itself. Whereas in our European concept, scientific institutions are independent of the state and their aim is the general advancement of scientific knowledge, which does not recognize state borders, in the PRC science is strictly subordinated to the pragmatic aims of the state, or rather the ruling Chinese Communist Party (CCP). This subordination of science to the interests of the state is institutionalized in the PRC.

Read the full article here.

UNIVERSITIES OPPOSE REQUEST TO HALT FOREIGN RECRUITMENT

Liz Newmark | University World News | January 21, 2023

Dutch universities are pushing back against an urgent request from Culture and Science Minister Robbert Dijkgraaf that universities and universities of applied sciences stop actively recruiting international students in international education fairs until further notice. University chairs have told University World News that the minister is taking a step too far. However, the universities themselves have proposed less restrictive curbs – such as an introduction of quotas on English tracks in degree programmes and limits on the proportion of international students in individual programmes. In a 22 December 2022 letter, sent to the university boards, Dijkgraaf demanded a halt to active recruitment given the pressure on staff, facilities and accommodation, "until new agreements are made in the context of Dijkgraaf's vision on internationalisation," according to the spokesperson for the Association of Universities in the Netherlands, Ruben Puylaert. "So, universities are not rejecting students, they have been asked to stop actively recruiting on study fairs," Puylaert explained.

Read the full article here.

TEXAS UNIVERSITIES BLOCK ACCESS TO TIKTOK ON CAMPUS WI-FI NETWORKS

Kate McGee | The Texas Tribune | January 17, 2023

The University of Texas at Austin has blocked access to the video-sharing app TikTok on its Wi-Fi and wired networks in response to Gov. Greg Abbott's recent directive requiring all state agencies to remove the app from government-issued devices, according to an email sent to students Tuesday. "The university is taking these important steps to eliminate risks to information contained in the university's network and to our critical infrastructure," UT-Austin technology adviser Jeff Neyland wrote in the email. "As outlined in the governor's directive, TikTok harvests vast amounts of data from its users' devices — including when, where and how they conduct internet activity — and offers this trove of potentially sensitive information to the Chinese government." Since the university's announcement Tuesday morning, multiple Texas university spokespeople, including those at the University of Texas at Dallas and Texas A&M University System, have announced they are also restricting the use of the app on their campus networks.

Read the full article here.

A U.S. DATA STRATEGY NET ASSESSMENT

Ylli Bajraktari, Rama Elluru, Chuck Howell, Jenilee Keefe Singer, and Ben Bain
Special Competitive Studies Project | January 9, 2023

We often think about measuring the state of the technology competition in terms of hardware innovation, nanometers, petaflops, or number of patents or PhDs trained. Assessing a nation's success in utilizing its data1 assets is more difficult, but equally important to the contest. How the United States and China use data to benefit their societies, accelerate their economies, and deliver for their citizens will go a long way toward determining how the contest between autocracies and democracies plays out over the long-run. Successful data utilization is not solely based on the amount of data available, but also on the rules, laws, and strategies that shape if and how data can be collected and used for productive purposes. The United States has more data centers than any other country, is home to the world's largest technology companies, dominates the big data and business analytics market, and is the world's largest data producer. But the United States has not effectively organized a whole-of-nation effort to fully leverage its massive government and non-government (private sector, academia, and civil society) data assets to gain a competitive advantage in the global contest with China.

Read the full article here.

INSIDER THREAT TASK FORCE PIVOTING FOCUS TO 'SAFEGUARDING SCIENCE'

Justin Doubleday | Federal News Network | September 27, 2022

The National Insider Threat Task Force is raising awareness about phishing, social engineering and other modern tactics used to target federal employees and contractors, while also gearing up for a new push aimed at "safeguarding science," according to its deputy director. The theme of year's "insider threat awareness month," held every September, has been "critical thinking in digital spaces." The task force and its partners have been highlighting online risks including social engineering efforts, mis-, dis-, and mal-information, and cyber tactics like phishing emails. Rebecca Morgan, assistant director for enterprise threat mitigation at the National Counterintelligence and Security Center and deputy director of the task force, says this year's campaign is motivated by the shift to remote work along with increasingly sophisticated online campaigns aimed at compromising the national security workforce.

Read the full article here.

WE NEED AN OPEN SOURCE INTELLIGENCE CENTER

Rodney Faraon and Peter Mattis | The Hill | January 20, 2023

In April 2018, Dutch authorities caught four Russian intelligence officers red-handed as they attempted to hack into the network of the Organization for the Prohibition of Chemical Weapons (OPCW) from the hotel across the street. The OPCW was investigating the substances used in the poisoning of a Russian defector living in the United Kingdom, and a chemical attack by Assad-backed forces in Douma, Syria. After the Dutch government publicly identified the four officers, open source researchers at Bellingcat — an independent investigative journalism group — leveraged the personal details of the four to identify 305 additional agents of the GRU, Russia's principal military intelligence unit. Bellingcat's researchers made the discovery using the agents' car registrations, which were linked to the service's training academy. This kind of open source discovery — once thought to be within the exclusive purview of governments — has become somewhat routine for skilled researchers in the private sector.

Read the full article here.

SEVEN (SCIENCE-BASED) COMMANDMENTS FOR UNDERSTANDING AND COUNTERING INSIDER THREATS

Eric L. Lang | Counter-Insider Threat Research and Practice | August 2, 2022

Organizational problems are rising. Serious data breaches, thefts of intellectual property (IP), and network compromises resulting from malicious, negligent, externally coerced, and well-meaning rule breakers within organizations have increased dramatically (Ponemon Institute, 2020; VentureBeat, 2022). Without effective management, such insider threats can undermine mission execution, employee safety, productivity, morale, financial stability, network functioning, asset integrity, public welfare, and local and global trust. "Insider threat" is an umbrella term covering the potential for "any person who has or had authorized access to, or knowledge of, an organization's assets and resources, to use their authorized access, wittingly or unwittingly, to bring harm to the organization's mission, resources, personnel, facilities, information, equipment, networks, or systems" (U.S. Cybersecurity & Infrastructure Security Agency, n.d.).

Read the full article here.

KNOWLEDGE SECURITY: INSIGHTS FOR NATO

David Snetselaar, Georg Frerks, Lauren Gould, Sebastiaan Rietjens, and Tim Sweijs | NATO Review | September 30, 2022

In the context of research on and the development of high-end technology, knowledge security is vital to NATO's ability to deter and defend against adversaries and protect the prosperity of its members. Countering hybrid threats that target critical national security technologies requires a whole-of-society approach that comprises the public sector, private companies, civil society and individuals aligning their principles and standards to engage meaningfully on an issue. The development of such an approach is hindered by diverging threat perceptions, interests and levels of awareness of the stakeholders (civilian and military; private and public) involved. To develop calibrated whole-of-society responses, NATO needs to understand what the opposing imperatives are for different stakeholders and how they can be bridged.

Read the full article here.