ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

March 9, 2022

ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

Office of the Director of National Intelligence | February 7, 2022

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the FY21 Intelligence Authorization Act (P.L. 116-260). This report reflects the collective insights of the Intelligence Community (IC), which is committed every day to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world. This assessment focuses on the most direct, serious threats to the United States during the next year. The order of the topics presented in this assessment does not necessarily indicate their relative importance or the magnitude of the threats in the view of the IC. All require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future, such as climate change and environmental degradation. As required by the law, this report will be provided to the congressional intelligence committees as well as the committees on the Armed Services of the House of Representatives and the Senate.

Read the full article here.

TECHNOLOGIES FOR AMERICAN INNOVATION AND NATIONAL SECURITY

White House Office of Science and Technology Policy | February 7, 2022

Today, the United States is releasing an updated list of critical and emerging technologies (CETs) that can play an important role in our nation's security. Last updated in 2020, this list represents a subset of novel, advanced technologies with the potential to chart new pathways in American innovation and strengthen our national security. The 2021 Interim National Security Strategic Guidance defines three national security objectives: (1) protect the security of the American people; (2) expand economic prosperity and opportunity; and (3) realize and defend democratic values. The 2021 CET list identifies the technology areas that currently hold the greatest potential to further those objectives in the future – and, for the first time, it also includes several specific subfields under each technology area. This list will be a useful resource that guides new and existing efforts to promote U.S. technological leadership, cooperate with allies and partners, advance democratic values, attract and retain diverse science and technology talent from around the world, and protect against threats to U.S. security.

Read the full article here.

EUROPEAN UNION HALTS SCIENTIFIC COOPERATION WITH RUSSIA

Brendan O'Malley | University World News | March 5, 2022

The European Commission has decided to halt cooperation with Russian entities in research, science and innovation in response to the Russian invasion of Ukraine, it announced on 4 March. As a result, the Commission will not conclude any new contracts nor any new agreements with Russian organisations under the European Union's flagship €95.5 billon research and innovation funding programme, Horizon Europe. In addition, the Commission is suspending payments to Russian entities under existing contracts. All ongoing projects, in which Russian research organisations are participating, are being reviewed – both under Horizon Europe and Horizon 2020, the previous EU programme for research and innovation. Since the Commission's announcement, the situation in Ukraine has deteriorated further, with Russian troops seizing the country's largest nuclear power plant, and shelling and bombarding a number of cities.

Read the full article here.

DOJ EMBOLDENS CHINA BY ENDING INITIATIVE AGAINST OUR GREATEST COUNTERINTELLIGENCE AND ECONOMIC ESPIONAGE THREAT

Michael Ellis | The Heritage Foundation | March 4, 2022

In November 2018, the Department of Justice (DOJ) launched a "China Initiative" to counter Chinese threats to U.S. national security. U.S. government policymakers had long discussed a "pivot to Asia" to confront China's increasingly aggressive behavior toward the United States, but little progress was made until President Donald J. Trump approved a National Security Strategy in December 2017. That strategy described the threat from China and stated that the United States would "prioritize counterintelligence and law enforcement activities to curtail intellectual property theft by all sources and will explore new legal and regulatory mechanisms to prevent and prosecute violations." The DOJ's China Initiative, which followed that change in U.S. government policy, sought to identify and prosecute trade secret theft, hacking, and economic espionage; protect U.S. critical infrastructure against threats from Chinese foreign direct investment and supply chain compromises; and combat covert efforts to influence the American public and policymakers.

Read the full article here.

ASSISTANT ATTORNEY GENERAL MATTHEW OLSEN DELIVERS REMARKS ON COUNTERING NATION-STATE THREATS

U.S. Department of Justice | February 23, 2022

Good afternoon. Thank you to the National Security Institute and George Mason University for inviting me. Unfortunately, my good friend Jamil Jaffer wasn't able to be here today. As I have told Jamil, I am so impressed with what you have built here at NSI. You all have a well-deserved reputation for taking on hard problems and developing practical solutions. Jamil and I first worked together in the brand new National Security Division more than 15 years ago. When NSD was established in 2006, I was the senior career official responsible for the Department of Justice's intelligence work. In November, I returned as the Assistant Attorney General for National Security. It is remarkable to see how the division has grown and what it has achieved over the years. And I am so proud to be leading NSD and its dedicated workforce now. As many of you know, Congress created NSD in the wake of the September 11th terrorist attacks. The idea was to unify and prioritize DOJ's national security work and to promote cooperation with the intelligence community and the broader national security community. In the years since, again and again, the work of NSD has proven critical to our national security.

Read the full article here.

USD(R&E) TECHNOLOGY VISION FOR AN ERA OF COMPETITION

Office of the Under Secretary of Defense, Research and Engineering | February 1, 2022

The Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E) will spearhead a National Defense Science and Technology strategy for the Department of Defense (DoD), informed by the 2022 National Defense Strategy (NDS) and structured around three strategic pillars: mission focus, foundation building, and succeeding through teamwork. This technology strategy will chart a course for the United States' military to strengthen its technological superiority amidst a global race for technological advantage. To maintain the United States military's technological advantage, the Department will champion research, science, technology, engineering, and innovation. From the earliest days of this country the role of technology in shaping military concepts and providing for the defense of the nation has been essential. The demands of the present era call for new operational concepts, increasingly joint operations, and quickly fielding emerging science and technology opportunities.

Read the full article here.

SECURING INTELLECTUAL PROPERTY FOR INNOVATION AND NATIONAL SECURITY

Sujai Shivakumar | Center for Strategic and International Studies | March 3, 2022

The United States is engaged in a global competition for innovation, with critical implications for the nation's continued technological leadership, competitiveness, and security. To win, the United States will need to leverage its advantages at home, including its robust intellectual property (IP) rights system and the innovative zeal of its entrepreneurs. It should also look abroad—setting the pace for scientific cooperation with allies and strategic partners, as well as developing shared international technical standards through the contributions of experts from around the globe. Most pressingly, the United States should not adopt policies that weaken protection of U.S.-owned patents—which would both disincentivize innovation in the United States and support Chinese efforts to dominate critical standards and other advanced technologies. Yet a recent proposal of the Antitrust Division of the U.S. Department of Justice (DOJ) does just that. Launched as a consultation, its Draft Policy Statement on Licensing Negotiations and

Read the full article here.

'I LOST TWO YEARS OF MY LIFE': US SCIENTIST FALSELY ACCUSED OF HIDING TIES TO CHINA SPEAKS OUT

Natasha Gilbert | Nature | March 7, 2022

Anming Hu walked back into his laboratory at the University of Tennessee (UT), Knoxville, on 1 February for the first time in about two years to find it stripped of research equipment. Gone were the delicate lasers, lenses and voltage metres — worth tens of thousands of dollars — that he and his students had used to conduct their studies. The nanotechnology researcher spent much of his first few weeks back at work searching for his prized tools. Some he found in colleagues' offices and labs, other pieces — some of them broken — he discovered packed into storage cupboards, he says. Others are still missing. "I want to get them back because those [are] my treasures," he says. Hu's tepid return to the university follows a turbulent few years during which he was accused by the US government of hiding ties with China, put under house arrest and, eventually, acquitted of all charges. This string of events occurred around the same time as the launch of the China Initiative — a US government effort to counter economic espionage that frequently targeted academic researchers for failing to disclose funds from China or partnerships with Chinese institutions.

Read the full article here.

US COURT CONVICTS RESEARCHER FOR SPYING ON US FOR RUSSIA

David Sun | University World News | March 6, 2022

Hector Alejandro Cabrera Fuentes (36), a scientist at Duke-NUS Medical School in Singapore, has authored more than 20 cardiology papers, and has also been linked to multiple academic institutions around the world. But the Mexican lived a double life with two wives, and was spying on the United States for Russia when he was in Miami, Florida, writes David Sun for The Straits Times. On 16 February, Fuentes pleaded guilty in an American court to spying on an informant in the US on behalf of the Russian government. The US Department of Justice said he had been acting under the direction and control of a Russian official to provide information on an informant who was providing information on Russia to the US government. Fuentes had spent significant time in Russia, having graduated from Kazan Federal University there in 2009, according to his LinkedIn page. He was employed by the National Heart Centre Singapore as a senior research fellow, and held a joint appointment in the cardiovascular and metabolic disorders programme at Duke-NUS Medical School. His services have since been terminated.

Read the full article here.

RUSSIA'S MOST CUTTHROAT HACKERS INFECT NETWORK DEVICES WITH NEW BOTNET MALWARE

Dan Goodin | Ars Technica | February 23, 2022

Hackers for one of Russia's most elite and brazen spy agencies have infected home and small-office network devices around the world with a previously unseen malware that turns the devices into attack platforms that can steal confidential data and target other networks. Cyclops Blink, as the advanced malware has been dubbed, has infected about 1 percent of network firewall devices made by network device manufacturer WatchGuard, the company said on Wednesday. The malware is able to abuse a legitimate firmware update mechanism found in infected devices in a way that gives it persistence, meaning the malware survives reboots. Cyclops Blink has been circulating for almost three years and replaces VPNFilter, the malware that in 2018 researchers found infecting about 500,000 home and small office routers. VPNFilter contained a veritable Swiss Army knife that allowed hackers to steal or manipulate traffic and to monitor some SCADA protocols used by industrial control systems. The US Department of Justice linked the hacks to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation, typically abbreviated as the GRU.

Read the full article here.

DAXIN: STEALTHY BACKDOOR DESIGNED FOR ATTACKS AGAINST HARDENED NETWORKS

Broadcom Software | February 28, 2022

New research by the Symantec Threat Hunter team, part of Broadcom Software, has uncovered a highly sophisticated piece of malware being used by China-linked threat actors, exhibiting technical complexity previously unseen by such actors. The malware appears to be used in a long-running espionage campaign against select governments and other critical infrastructure targets. There is strong evidence to suggest the malware, Backdoor.Daxin, which allows the attacker to perform various communications and data-gathering operations on the infected computer, has been used as recently as November 2021 by attackers linked to China. Most of the targets appear to be organizations and governments of strategic interest to China. In addition, other tools associated with Chinese espionage actors were found on some of the same computers where Daxin was deployed. Daxin is without doubt the most advanced piece of malware Symantec researchers have seen used by a China-linked actor.

Read the full article here.

BIDEN TERMINATES CHINA PROBE 'DUE TO IMPACT ON SCIENCE'

Nathan M. Greenfield | University World News | February 25, 2022

Citing the "rise in anti-Asian hate crime and hate incidents" in the United States and the fact that the prosecutions of American scholars of Chinese descent for research grant fraud has created a "chilling narrative for scientists and scholars that damages the scientific enterprise in this country", Assistant Attorney General Matthew Olsen announced the end of the China Initiative on 23 February. "I want to emphasise," Olsen told an audience at George Mason University in Washington DC that included members from the National Security Institute, that the Department of Justice's (DOJ's) "actions have been driven by genuine national security concerns" about covert influence by China, including theft of trade secrets, cutting-edge semiconductor technology, seeds developed for pharmaceutical uses, malicious cyber activity and transnational repression (of Chinese studying or working in the United States).

Read the full article here.

MORE UNIVERSITIES BECOME 'WORLD CLASS' TO MEET CHINA AMBITIONS

Yojana Sharma | University World News | February 17, 2022

China has expanded its list of world-class universities, adding seven new institutions to the 140 that will receive special funding for teaching and research in specific subject areas and other benefits to compete with the world's major universities. The action was billed as the second phase of the 'double first-class' university programme following the initial phase that began in 2016 and ended in 2020, in a joint announcement this week by the Ministry of Education, the Finance Ministry and the economic planning agency the National Development and Reform Commission under the State Council, which is roughly equivalent to cabinet. The announcement noted that despite "remarkable results promoting the building of a powerful higher education nation", there was still insufficient throughput of "high-level innovation talents" from universities.

Read the full article here.

ANALYZING CHINA'S RESEARCH COLLABORATION WITH THE UNITED STATES IN HIGH-IMPACT AND HIGH-TECHNOLOGY RESEARCH

Yongjun Zhu, Donghun Kim, Erjia Yan, Meen Chul Kim, Guanqiu Qi | MIT Press Direct | April 8, 2021

This study investigates China's international research collaboration with the United States through a bibliometric analysis of coauthorship over time using historical research publication data. We investigate from three perspectives: overall, high-impact, and high-technology research collaborations using data from Web of Science (WoS), Nature Index, and Technology Alert List maintained by the U.S. Department of State. The results show that the United States is China's largest research collaborator and that in all three aspects, China and the United States are each other's primary collaborators much of the time. From China's perspective, we have found weakening collaboration with the United States over the past 2 years. In terms of high-impact research collaboration, China has historically shared a higher percentage of its research with the United States than vice versa.

Read the full article here.