ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

July 7, 2021

RETIRED GERMAN POLITICAL SCIENTIST CHARGED WITH SPYING FOR CHINA

Reuters | July 6, 2021

A retired German political scientist has been charged with spying for China for almost a decade, using the political contacts he developed while working for a think tank, the German federal prosecutor's office said on Tuesday. It said the man, identified as Klaus L. according to German reporting custom, had been recruited during a lecture trip to Shanghai in 2010, almost 10 years after joining the think tank, and had regularly passed on information until November 2019, in return for money and trips to China. The public broadcaster ARD said Klaus L. had also been a spy for Germany's foreign intelligence agency, the BND, for half a century before retiring. ARD cited unnamed sources as saying he had initially told the BND of the recruitment attempt, but had failed to inform it about later contacts. ARD also said Klaus L. had worked for the Munich-based Hanns Seidel Foundation, associated with the Christian Social Union (CSU), Bavarian sister party to Chancellor Angela Merkel's CDU.

Read the full article here.

CHINA'S NATIONAL CYBERSECURITY CENTER: A BASE FOR MILITARY-CIVIL FUSION IN THE CYBER DOMAIN

Dakota Cary | Center for Security and Emerging Technology | July 2021

China wants to be a "cyber powerhouse" (网络强国). At the heart of this mission is the sprawling 40 km2 campus of the National Cybersecurity Center. Formally called the National Cybersecurity Talent and Innovation Base (国家网络安全人才与创新基地), the NCC is being built in Wuhan. The campus, which China began constructing in 2017 and is still building, includes seven centers for research, talent cultivation, and entrepreneurship; two government-focused laboratories; and a National Cybersecurity School. The NCC enjoys support from the highest levels of the Chinese Communist Party (CCP). The Party's Cyberspace Affairs Commission established a committee to oversee the NCC's operations and policies, giving it a direct line to Beijing. International competition forged China's commitment to growing its cyber capabilities. Despite a deficit of 1.4 million cybersecurity professionals, China is already a near-peer cyber power to the United States. Still, the current shortfall leaves China's businesses and infrastructure vulnerable to attack, while spreading thin its offensive talent.

Read the full report here.

NSA, PARTNERS RELEASE CYBERSECURITY ADVISORY ON BRUTE FORCE GLOBAL CYBER CAMPAIGN

National Security Agency Central Security Service | July 1, 2021

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and the UK's National Cyber Security Centre (NCSC) released a Cybersecurity Advisory today exposing malicious cyber activities by Russian military intelligence against U.S. and global organizations, starting from mid-2019 and likely ongoing. This advisory is being released as part of NSA's routine and continuing cybersecurity mission to warn network defenders of nation state threats. "Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments" details how the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) has targeted hundreds of U.S. and foreign organizations using brute force access to penetrate government and private sector victim networks. The advisory reveals the tactics, techniques, and procedures (TTPs) GTsSS actors used in their campaign to exploit targeted networks, access credentials, move laterally, and collect and exfiltrate data. It also arms system administrators with the mitigations needed to counter this threat.

Read the full article here.

"THEY DON'T UNDERSTAND THE FEAR WE HAVE": HOW CHINA'S LONG REACH OF REPRESSION UNDERMINES ACADEMIC FREEDOM AT AUSTRALIA'S UNIVERSITIES

Sophie McNeill | Human Rights Watch | June 30, 2021

In 2020, nearly 160,000 students from China were enrolled in Australian universities. Despite the Chinese government in Beijing being thousands of kilometers away, many Chinese pro-democracy students in Australia say they alter their behavior and self-censor to avoid threats and harassment from fellow classmates and being "reported on" by them to authorities back home. Students and academics from or working on China told Human Rights Watch that this atmosphere of fear has worsened in recent years, with free speech and academic freedom increasingly under threat. The Chinese government has grown bolder in trying to shape global perceptions of the country on foreign university campuses, influence academic discussions, monitor students from China, censor scholarly inquiry, or otherwise interfere with academic freedom.

Read the full article here.

NSA-CISA-NCSC-FBI JOINT CYBERSECURITY ADVISORY ON RUSSIAN GRU BRUTE FORCE CAMPAIGN

National Security Agency, Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and United Kingdom National Cyber Security Centre | July 1, 2021

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and the UK's National Cyber Security Centre (NCSC) have released Joint Cybersecurity Advisory (CSA): Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments. The CSA provides details on the campaign, which is being conducted by the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS). The campaign uses a Kubernetes® cluster in brute force access attempts against the enterprise and cloud environments of government and private sector targets worldwide.

Read the full article here.

ATTACKERS USE 'OFFENSIVE AI' TO CREATE DEEPFAKES FOR PHISHING CAMPAIGNS

Kyle Wiggers | Venture Beat | July 2, 2021

AI enables organizations to automate tasks, extract information, and create media nearly indistinguishable from the real thing. But like any technology, AI isn't always leveraged for good. In particular, cyberattackers can use AI to enhance their attacks and expand their campaigns. A recent survey published by researchers at Microsoft, Purdue, and Ben-Gurion University, among others, explores the threat of this "offensive AI" on organizations. It identifies different capabilities that adversaries can use to bolster their attacks and ranks each by severity, providing insights on the adversaries. The survey, which looked at both existing research on offensive AI and responses from organizations including IBM, Airbus, Airbus, IBM, and Huawei, identifies three primary motivations for an adversary to use AI: coverage, speed, and success.

Read the full article here.

MORE THAN INNOVATION AND COMPETITION: THE LATEST PROPOSED MONITORING AND ENFORCEMENT MECHANISMS TARGETING FOREIGN INFLUENCE IN U.S. RESEARCH

Christopher Nasson, Scott Ofrias, David Peet, David Rybicki, & Rebecca Schaefer | JD Supra | July 2, 2021

On 8 June 2021, the Senate passed an expansive bipartisan bill aimed at enhancing the country's scientific research and development capabilities. In response to emerging technological competition from foreign innovation sources, the U.S. Innovation & Competition Act (USICA) contemplates devoting US$250 billion to the National Science Foundation, thereby ensuring that the United States maintains its "position as the most innovative and productive nation on Earth." Yet this recent bill is more than just a financial incentive to innovate. Importantly for funding recipients, including research institutions and academic medical centers, this legislation contains significant research security measures to safeguard American technology and intellectual property. These proposed measures would formally exclude researchers who participate in foreign talent recruitment programs from participating in federally funded research projects.

Read the full article here.

UNDERSTANDING INFLUENCE IN THE STRATEGIC COMPETITION WITH CHINA

Michael J. Mazarr, Bryan Frederick, John J. Drennan, Emily Ellinger, Kelly Elizabeth Eusebi, Bryan Rooney, Andrew Stravers, Emily Yoder | RAND | 2021

Over the past two decades, China's role in the geopolitical landscape has grown, particularly as a result of the country's rising economic and military power. Thus, U.S. leaders now view China as a strategic competitor—one that seeks to upend the post–World War II liberal international order. One of China's strategies in that competition is to seek influence in countries around the world. In this report, the authors assess China's ability to use various mechanisms of influence to shape the policies and behavior of 20 countries, as well as the lessons that these examples offer for the United States' strategic competition with China. With this study, the authors aim to produce a transferable framework (comprising inputs, intervening factors, and outputs) and other tools of analysis that can provide reliable means of assessing bilateral influence relationships in other cases. Among the study's chief findings is that China's burgeoning economic power, above and beyond any other considerations, is the foundation for its influence.

Read the full article here.

WHAT THE U.S. INNOVATION AND COMPETITION ACT GETS RIGHT (AND WHAT IT GETS WRONG)

Jake Harrington and Riley McCabe | Center for Strategic and International Studies | July 1, 2021

The Senate's recent adoption of the U.S. Innovation and Competition Act sent an important message that, even in a deeply divided Washington, challenging China's efforts to displace the United States as the world's technology superpower is an increasingly bipartisan issue. Although the bill—if passed by the House—would authorize a welcome boost of $250 billion of investment in a range of emerging technologies, this figure represents a mere drop in the bucket compared to the trillions that Beijing continues to pour into its own technology development. Simply put, the United States cannot and should not attempt to compete with China in a race of state-backed investments. Indeed, what could prove more valuable than the price tag of the Innovation and Competition Act is a series of counterintelligence and security enhancements intended to protect U.S. innovation and strengthen national competitiveness.

Read the full article here.

XI JINPING'S COMPLICATED QUEST FOR THE STATE-CORPORATE TECHNOLOGY COMPLEX

Ngor Luong | The Diplomat | June 28, 2021

The relationship between the Chinese government and its private tech sector can appear mystifying. Beijing seems to be asserting more control over Chinese tech giants, for example, by cracking down on Alibaba and Tencent for growing too powerful. At the same time, the Chinese leadership recognizes that it must also allow some degree of independence for firms to be efficient and profitable. To China's leaders, this position is not paradoxical. As Xi Jinping recently remarked, "We encourage the development of private businesses. When they encounter difficulties [and] confusion arises," the Chinese Communist Party (CCP) provides "guidance" so that "they can develop boldly and with confidence." What constitutes "difficulties" is up to the CCP to decide, and so are the methods for course correction when private firms are "confused." To put this idea into practice, the government is taking the carrot-and-stick approach.

Read the full article here.

ALL CANADIAN UNIVERSITIES MUST CRITICALLY REASSESS THEIR COLLABORATIONS WITH CHINA | INSTITUTE FOR SCIENCE, SOCIETY AND POLICY | UNIVERSITY OF OTTAWA

Margaret McCuaig-Johnston | University of Ottawa | June 29, 2021

Canada is proud to have one of the world's best research environments for cutting-edge development in technology and science. But recent media reports have documented the risks of a system where Canadian researchers may collaborate with China. As the new China of President Xi Jinping has become more aggressive in acquiring technology from other countries, we have found that China's military scientists – as well as companies implicated in the regime's surveillance state, such as iFlytek, SenseTime, Alibaba and BGI Group – have established research relationships with Canada's top universities and research centres. Canadian researchers partnering with colleagues in China in areas such as artificial intelligence, nanotechnology, biotechnology, photonics, quantum computing and advanced materials may not realize that their great ideas shared with Chinese colleagues may be going out the back door into military applications. Mr. Xi's ramped-up policy to integrate civilian and military technology development means Chinese civilian scientists cannot refuse to partner with their military counterparts.

Read the full article here.

CHINESE STUDENTS FEAR REPRISALS FROM THEIR OWN GOVERNMENT

Geoff Maslen | University World News | July 1, 2021

Almost 160,000 students from China were enrolled in Australian universities in 2020. But, despite being thousands of kilometres from home, many Chinese students modified their normal behaviour and 'self-censored', according to a new study reported by Human Rights Watch, the New York-based international human rights organisation. Broadly aware that the Chinese government carries out surveillance in Australian universities of pro-democracy students from mainland China and Hong Kong, they censored themselves both to avoid threats and harassment from their Chinese classmates and because they feared being named in reports to authorities back home. Academics whose work focuses on China have adopted self-censorship, the report says. The Human Rights Watch report, They Don't Understand the Fear we Have: How China's long reach of repression undermines academic freedom at Australia's universities, found that this atmosphere of fear had worsened in recent years, with free speech and academic freedom increasingly under threat.

Read the full article here.

MORE THAN INNOVATION AND COMPETITION: THE LATEST PROPOSED MONITORING AND ENFORCEMENT MECHANISMS TARGETING FOREIGN INFLUENCE IN U.S. RESEARCH

David Peet, Christopher L. Nasson, David C. Rybicki, Rebecca M. Schaefer, and Scott G. Ofrias
The National Law Review | July 1, 2021

On 8 June 2021, the Senate passed an expansive bipartisan bill aimed at enhancing the country's scientific research and development capabilities. In response to emerging technological competition from foreign innovation sources, the U.S. Innovation & Competition Act (USICA) contemplates devoting US$250 billion to the National Science Foundation, thereby ensuring that the United States maintains its "position as the most innovative and productive nation on Earth." Yet this recent bill is more than just a financial incentive to innovate. Importantly for funding recipients, including research institutions and academic medical centers, this legislation contains significant research security measures to safeguard American technology and intellectual property. These proposed measures would formally exclude researchers who participate in foreign talent recruitment programs from participating in federally funded research projects.

Read the full article here.

CHINA PRESSURE 'UNDERMINING AUSTRALIAN UNIVERSITIES', REPORT SAYS

BBC News | June 30, 2021

Chinese pro-democracy students in Australia experience harassment and fear punishment if they speak out on sensitive issues, a new report says. Human Rights Watch found such students feel surveilled in Australia, leading many to self-censor in classrooms. Academics teaching China courses in the country say they have also felt pressure to censor themselves. China's embassy in Canberra strongly rejected the report on Wednesday, calling it "biased". It said Human Rights Watch had "decayed into a political tool for the West" and the group was "always biased on China". The Australian government said it found the report "deeply concerning". There has been growing concern about China's influence on local campuses in recent years, following a deterioration in relations between the two nations. Canberra is already investigating allegations of potential foreign interference.

Read the full article here.

RESEARCH SECURITY, COLLABORATION, AND THE CHANGING MAP OF GLOBAL R&D

Melissa Flagg, Autumn Toney, and Paul Harris | Georgetown University Center for Security and Emerging Technology | June 2021

The global map of research has shifted dramatically over the last 20 years. Annual global investment in research and development has tripled and the United States' share of global R&D funding and total research output is diminishing. The open research system, with its expanding rates of investment and interconnectedness, has delivered tremendous benefits to many nations, but it has also created new challenges to research integrity and security. Our data shows significant variations across countries in how much, and in what ways, they rely on their collaborative links to the global research network. A more nuanced understanding of those differences is critical for assessing the unique cost/benefit calculations behind decisions to limit open engagement to address security concerns.

Read the full article here.

JULY 4TH RANSOMWARE ATTACK MAY BE THE LARGEST EVER - EXPERT

Zev Stub | The Jerusalem Post | July 4, 2021

This attack is different from the SolarWinds attack, which exposed sensitive data from government offices and thousands of private companies in what is possibly the largest security breach ever. A ransomware attack by the Russian-based REvil gang on the eve of the July 4th US holiday weekend may end up being even larger than the recent SolarWinds hack, an Israeli cybersecurity expert has told The Jerusalem Post. The supply-chain attack on IT management software provider Kaseya has been under-reported in the media due to the holiday, but may set a new precedent for future cyberattacks, said Demi Ben-Ari, Co-Founder & CTO of Tel Aviv-based security management company Panorays. Kaseya provides IT management tools for some 40,000 customers worldwide. The company has said that REvil managed to target only about 40 of its clients, but that some of those are Managed Service Providers (MSPs) that may each work with hundreds of businesses.

Read the full article here.

COMPARING THE UNITED STATES' AND CHINA'S LEADING ROLES IN THE LANDSCAPE OF SCIENCE

Autumn Toney and Melissa Flagg | Georgetown University Center for Security and Emerging Technology June 2021

Research output is a frequently used index to assess the global competition for leadership in science and technology (S&T). This competition—among countries as well as institutions—leads to challenging questions: Which countries are leading in publication output? Which institutions are producing the most influential research? Which organizations are investing the most in research? These questions are frequently addressed with broad overviews of the research landscape, but a focused analysis on subsets of research provides more nuanced and accurate comparisons. While one entity may appear to dominate in a broad area of research, it might fall in the ranks when the research area is broken down into subsets. To explore country-level research output at varying levels of granularity, we navigate the landscape via CSET's recently developed Map of Science. Using this clustering of scientific research publications that is sourced from a massive database, we analyze scientific publication output at three different levels of aggregation: 1) research clusters, 2) research regions, and 3) research districts.

Read the full article here.

BIS 'RESCINDS IDENTIFICATION OF TIKTOK/WECHAT PROHIBITED TRANSACTIONS'

World ECR | June 24, 2021

In a notice in the Federal Register published 23 June, the US Bureau of Industry and Security ('BIS') announced that 'pursuant to Executive Order 14034 of June 9, 2021….the Secretary of Commerce has rescinded two actions issued under now-revoked Executive Orders: The September 18, 2020 Identification of Prohibited Transactions related to TikTok, published on September 24, 2020, and the September 18, 2020 Identification of Prohibited Transactions related to WeChat filed for public inspection on September 18, 2020 and withdrawn before publication. The notice explains the background and history of the earlier executive orders and adds: 'On June 9, 2021, Executive Order 14034 (Protecting Americans' Sensitive Data from Foreign Adversaries) revoked Executive Orders 13942 and 3943 and required executive departments and agencies to promptly take steps to rescind any orders, rules, regulations, guidelines, or policies, or portions thereof, implementing or enforcing those Executive Orders (86 FR 31423). Accordingly, the Secretary of Commerce has rescinded the Identification of Prohibited Transactions with respect to TikTok and the Identification of Prohibited Transactions with respect to WeChat.'

Read the full article here.