ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

December 23, 2020

THE INFLUENCE ENVIRONMENT

Alex Joske, Lin Li, Alexandra Pascoe, and Nathan Attrill | Australian Strategic Policy Institute
December 17, 2020

In the past two decades, Australia's Chinese-language media landscape has undergone fundamental changes that have come at a cost to quality, freedom of speech, privacy and community representation. The diversity of Australia's Chinese communities, which often trace their roots to Hong Kong, Southeast Asia and Taiwan as well as the People's Republic of China, isn't well reflected in the media sector. Persistent efforts by the Chinese Communist Party (CCP) to engage with and influence Chinese language media in Australia far outmatch the Australian Government's work in the same space. A handful of outlets generally offer high-quality coverage of a range of issues. However, CCP influence affects all media. It targets individual outlets while also manipulating market incentives through advertising, coercion and WeChat. Four of the 24 Australian media companies studied in this report show evidence of CCP ownership or financial support.

Read the full article here.

CHINA USED STOLEN DATA TO EXPOSE CIA OPERATIVES IN AFRICA AND EUROPE

Zach Dorfman | Foreign Policy | December 21, 2020

Around 2013, U.S. intelligence began noticing an alarming pattern: Undercover CIA personnel, flying into countries in Africa and Europe for sensitive work, were being rapidly and successfully identified by Chinese intelligence, according to three former U.S. officials. The surveillance by Chinese operatives began in some cases as soon as the CIA officers had cleared passport control. Sometimes, the surveillance was so overt that U.S. intelligence officials speculated that the Chinese wanted the U.S. side to know they had identified the CIA operatives, disrupting their missions; other times, however, it was much more subtle and only detected through U.S. spy agencies' own sophisticated technical countersurveillance capabilities. The CIA had been taking advantage of China's own growing presence overseas to meet or recruit sources, according to one of these former officials. "We can't get to them in Beijing, but can in Djibouti. Heat map Belt and Road"—China's trillion-dollar infrastructure and influence initiative—"and you'd see our activity happening. It's where the targets are." The CIA recruits "Russians and Chinese hard in Africa," said a former agency official. "And they know that." China's new aggressive moves to track U.S. operatives were likely a response to these U.S. efforts.

Read the full article here.

AGENCIES NEED TO ENHANCE POLICIES TO ADDRESS FOREIGN INFLUENCE

U.S. Government Accountability Office | December 17, 2020

U.S. research may be subject to undue foreign influence in cases where a researcher has a foreign conflict of interest (COI). Federal grant-making agencies can address this threat by implementing COI policies and requiring the disclosure of information that may indicate potential conflicts. GAO reviewed five agencies—which together accounted for almost 90 percent of all federal research and development expenditures at universities in fiscal year 2018—and found that three have agency-wide COI policies, while two do not (see figure). The three agencies with existing policies focus on financial interests but do not specifically address or define non-financial interests, such as multiple professional appointments. In the absence of agency-wide COI policies and definitions on non-financial interests, researchers may not fully understand what they need to report on their grant proposals, leaving agencies with incomplete information to assess the risk of foreign influence.

Read the full article here.

CHINA-BASED EXECUTIVE AT U.S. TELECOMMUNICATIONS COMPANY CHARGED WITH DISRUPTING VIDEO MEETINGS COMMEMORATING TIANANMEN SQUARE MASSACRE

U.S. Department of Justice | December 18, 2020

A complaint and arrest warrant were unsealed today in federal court in Brooklyn charging Xinjiang Jin, also known as "Julien Jin," with conspiracy to commit interstate harassment and unlawful conspiracy to transfer a means of identification. Jin, an employee of a U.S.-based telecommunications company (Company-1) who was based in the People's Republic of China (PRC), allegedly participated in a scheme to disrupt a series of meetings in May and June 2020 held to commemorate the June 4, 1989 Tiananmen Square massacre in the PRC. The meetings were conducted using a videoconferencing program provided by Company-1, and were organized and hosted by U.S-based individuals, including individuals residing in the Eastern District of New York. Jin is not in U.S. custody. "No company with significant business interests in China is immune from the coercive power of the Chinese Communist Party," said Assistant Attorney General for National Security John C. Demers.

Read the full article here.

DEFEND LIKEMINDED ALLIES AND PARTNERS AND THE RULES-BASED SYSTEM FROM CHINA AND IMPOSE COSTS ON CHINA WHEN IT VIOLATES INTERNATIONAL STANDARDS

Jeffrey Cimmino and Matthew Kroenig | Atlantic Council | December 16, 2020

Likeminded allies and partners should defend against China's unfair economic practices. The economies of likeminded allies and partners and China have become highly interdependent, with significant flows of trade, finance, and cross-national production across their borders. There is currently a debate in the United States about whether the United States should "decouple" from the Chinese economy. Proponents argue that the national security risks of continued economic engagement outweigh the risks, while opponents maintain that the economic costs of decoupling would be catastrophic and could increase the risk of geopolitical conflict. This strategy paper advocates approaching decoupling with a scalpel rather than a machete, and recognizes four discrete categories of economic engagement.

Read the full article here.

AN AUSTRALIAN STUDENT DENOUNCED HIS UNIVERSITY'S TIES TO CHINA. THEN HE BECAME A TARGET

Shashank Bengali and Maria Petrakis | Los Angeles Times | December 21, 2020

Before the text messages threatening to kill his family, Drew Pavlou gathered a small group of students on a busy walkway at the University of Queensland to protest the Chinese government's repression of Uighur Muslims and crackdown on Hong Kong. "Hey-hey, ho-ho — Xi Jinping has got to go!" As he denounced the Communist leader, hundreds of counter-demonstrators massed around a colonnade at the campus in Brisbane, Australia. Some were students from China; others appeared older. They yelled pro-Beijing slogans and played the Chinese national anthem over loudspeakers. Pavlou, 20, stopped for a moment and smiled, relishing the first protest he'd ever organized. Things quickly turned violent. A man in the crowd rushed at Pavlou, snatching his megaphone. A second man shoved him. In the ensuing scuffles, one student from Hong Kong was tackled and grabbed by the throat; another had her shirt ripped open.

Read the full article here.

I WAS THE HOMELAND SECURITY ADVISER TO TRUMP. WE'RE BEING HACKED.

Thomas P. Bossert | The New York Times | December 16, 2020

At the worst possible time, when the United States is at its most vulnerable — during a presidential transition and a devastating public health crisis — the networks of the federal government and much of corporate America are compromised by a foreign nation. We need to understand the scale and significance of what is happening. Last week, the cybersecurity firm FireEye said it had been hacked and that its clients, which include the United States government, had been placed at risk. This week, we learned that SolarWinds, a publicly traded company that provides software to tens of thousands of government and corporate customers, was also hacked. The attackers gained access to SolarWinds software before updates of that software were made available to its customers. Unsuspecting customers then downloaded a corrupted version of the software, which included a hidden back door that gave hackers access to the victim's network. This is what is called a supply-chain attack, meaning the pathway into the target networks relies on access to a supplier.

Read the full article here.

UNIVERSITIES WARN FOREIGN INTERFERENCE MEASURES MUST BE 'CAREFULLY CALIBRATED'

Lisa Visentin | The Sydney Morning Herald | December 21, 2020

Australia's elite research universities have warned that partnerships with Chinese institutions, including those which have led to world-leading research developments, could be jeopardised if the Morrison government fails to carefully calibrate foreign interference measures. The Group of Eight, which represents the eight universities that account for 70 per cent of academic research, says the collaboration of University of Sydney professor Edward Holmes in the first genome sequencing of COVID-19 – a project involving a consortium of Chinese universities and institutions – is a key example of research that "might not have occurred" under stricter policy settings. It also highlighted as another example the work of Monash University Professor Paul Zimmet AO in an international team, which included Peking University Professor Linong Ji, that found that elderly people with diabetes who contracted COVID-19 faced a much higher risk of dying. The examples were detailed in a submission to a federal parliamentary inquiry into national security risks affecting the higher education and research sector.

Read the full article here.

CHINA REPORTEDLY SPYING ON 'TENS OF THOUSANDS' OF AMERICANS VIA CELLPHONES

Paul Wagenseil | Tom's Guide | December 22, 2020

China has been using telephone companies in the Bahamas and Barbados to spy on "tens of thousands" of American citizens, a mobile-phone security expert told Britain's Guardian newspaper. "The attacks qualify as mass surveillance, which is primarily for intelligence collection and not necessarily targeting high-profile targets," said Gary Miller, founder of Exigent Media, a Seattle-area media-production company specializing in cybersecurity issues. "These occur primarily while people are [traveling] abroad." The Guardian article does not get into technical details, but a two-part report entitled "Far from Home" posted on the Exigent Media website makes clear that Miller is talking about abuses of the Signaling System 7 (SS7) telephone-signaling network and its successor, the Diameter signaling protocol. The report details "a comprehensive vision into foreign surveillance attacks and cyber espionage threat activity against U.S. mobile phones."

Read the full article here.

NUCLEAR WEAPONS AGENCY BREACHED AMID MASSIVE CYBER ONSLAUGHT

Natasha Bertrand and Eric Wolff | Politico | December 17, 2020

The Energy Department and National Nuclear Security Administration, which maintains the U.S. nuclear weapons stockpile, have evidence that hackers accessed their networks as part of an extensive espionage operation that has affected at least half a dozen federal agencies, officials directly familiar with the matter said. On Thursday, DOE and NNSA officials began coordinating notifications about the breach to their congressional oversight bodies after being briefed by Rocky Campione, the chief information officer at DOE. They found suspicious activity in networks belonging to the Federal Energy Regulatory Commission (FERC), Sandia and Los Alamos national laboratories in New Mexico and Washington, the Office of Secure Transportation at NNSA, and the Richland Field Office of the DOE. The hackers have been able to do more damage at FERC than the other agencies, and officials there have evidence of highly malicious activity, the officials said, but did not elaborate. The officials said that the Cybersecurity and Infrastructure Security Agency, which has been helping to manage the federal response to the broad hacking campaign, indicated to FERC this week that CISA was overwhelmed and might not be able to allocate the necessary resources to respond.

Read the full article here.

INTELLIGENCE THREATS & SOCIAL MEDIA DECEPTION

Office of the Director of National Intelligence | The National Counterintelligence and Security Center

Do you want to connect? Understand that foreign intelligence entities and criminals routinely use deception on social media platforms to try and connect with people who have access to information they want. Before you link online with someone you don't know, think about the risks it may pose to yourself, your family, your organization and even national security. The FBI and the National Counterintelligence and Security Center (NCSC) have released a new movie, "The Nevernight Connection," to raise awareness of how hostile actors use fake profiles and other forms of deception on social media to target individuals in government, business and academic communities for recruitment and information gathering. Inspired by true events, the 30-minute video details the fictional account of a former U.S. Intelligence Community official targeted by a foreign intelligence service via a fake profile on a professional networking site and recruited to turn over classified information.

Read the full article here.

DEFENSE ACQUISITIONS: DOD'S CYBERSECURITY MATURITY MODEL CERTIFICATION FRAMEWORK

Heidi M. Peters | Congressional Research Service | December 18, 2020

Cybersecurity threats represented by cyberattacks and data theft have had a significant impact on the Department of Defense (DOD) and the defense industrial base (DIB). These threats have become a significant concern to policymakers due to recent alleged incidents involving the unlawful acquisition of significant quantities of sensitive defense information from DIB systems. As part of its response to these threats, DOD began work in early 2019 to develop the Cybersecurity Maturity Model Certification (CMMC) framework. This DOD-driven initiative intends to provide a "unified cybersecurity standard" for defense acquisitions and aims to use and build on existing law and regulations. Once fully in place, the CMMC framework would establish a "verification mechanism" requiring all prime contractors and subcontractors seeking to do business with the DOD to obtain certification from accredited third-party organizations that contractors' in-house cybersecurity practices and processes meet certain standards.

Read the full article here.

COUNTERING RUSSIAN & CHINESE INFLUENCE ACTIVITIES

Heather A. Conley, Rachel Ellehuus, Timothy Kostelancik, Jeffrey Mankoff, Cyrus Newlin, Amy Searight, and Devin Stewart | Center for Strategic & International Studies

The impact of Russian and Chinese malign influence activities within democratic states has come into sharp focus in recent years. In 2020, the Covid-19 pandemic has created new opportunities for Moscow and Beijing to advance geopolitical goals through disinformation and other influence activities. Despite greater public awareness of the challenge, governments have struggled to respond. The "3 Cs" framework, coined by former Australian Prime Minister Malcolm Turnbull, defines "malign" influence activities as covert, coercive, or corrupting. These influence activities disrupt the normal democratic political processes in a targeted country by: 1. Manipulating public discourse; 2. Discrediting the electoral system; 3. Biasing the development of policy; or 4. Disrupting markets for the purpose of advancing a political or strategic goal. These activities are typically non-transparent, outside the rule of law, and run counter to liberal democratic norms. Activities that are covert, coercive, or corrupting differ from legitimate or benign public diplomacy efforts conducted in a transparent and open manner.

Read the full article here.

GAO: AGENCIES SHOULD DO MORE TO PROTECT SCIENTIFIC RESEARCH FROM FOREIGN INFLUENCE

Kylie Bielby | Homeland Security Today | December 19, 2020

To protect U.S. investments in scientific research from undue foreign influence, federal agencies should have conflict of interest (COI) policies and require researchers to disclose foreign interests. But a Government Accountability Office (GAO) review has found that not all federal agencies have agency-wide financial conflict of interest policies. U.S. research may be subject to undue foreign influence in cases where a researcher has a foreign COI. Federal grant-making agencies can address this threat by implementing COI policies and requiring the disclosure of information that may indicate potential conflicts. The National Defense Authorization Act for Fiscal Year 2020 (FY 2020 NDAA) included a requirement for an interagency working group to "coordinate activities to protect federally funded research and development from foreign interference, cyber-attacks, theft, or espionage and to develop common definitions and best practices for federal science agencies and grantees."

Read the full article here.

ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY

Kelley M. Sayler and Daniel S. Hoadley | Congressional Research Service | November 10, 2020

Artificial intelligence (AI) is a rapidly growing field of technology with potentially significant implications for national security. As such, the United States and other nations are developing AI applications for a range of military functions. AI research is underway in the fields of intelligence collection and analysis, logistics, cyber operations, information operations, command and control, and in a variety of semiautonomous and autonomous vehicles. Already, AI has been incorporated into military operations in Iraq and Syria. Congressional action has the potential to shape the technology's development further, with budgetary and legislative decisions influencing the growth of military applications as well as the pace of their adoption. AI technologies present unique challenges for military integration, particularly because the bulk of AI development is happening in the commercial sector. Although AI is not unique in this regard, the defense acquisition process may need to be adapted for acquiring emerging technologies like AI. In addition, many commercial AI applications must undergo significant modification prior to being functional for the military. A number of cultural issues also challenge AI acquisition, as some commercial AI companies are averse to partnering with the Department of Defense (DOD) due to ethical concerns, and even within the department, there can be resistance to incorporating AI technology into existing weapons systems and processes.

Read the full article here.

INTELLECTUAL PROPERTY PROTECTION: 10 TIPS TO KEEP IP SAFE

Alyson Behr and Derek Slater | CSO | February 28, 2019

Intellectual property (IP) is the lifeblood of every organization. It didn't used to be. As a result, now more than ever, it's a target, placed squarely in the cross-hairs by various forms of cyber attack. Witness the long list of hacks on Hollywood and the entertainment industry's IP including "Pirates of the Caribbean" and more recently HBO's "Game of Thrones." Your company's IP, whether that's patents, trade secrets or just employee know-how, may be more valuable than its physical assets. Security pros must understand the dark forces that are trying to get this information from your company and piece it together in a useful way. Some of these forces come in the guise of "competitive intelligence" researchers who, in theory, are governed by a set of legal and ethical guidelines carefully wrought by the Society of Competitive Intelligence Professionals (SCIP). Others are outright spies hired by competitors, or even foreign governments, who'll stop at nothing, including bribes, thievery, or even a pressure-activated tape recorder hidden in your CEO's chair.

Read the full article here.