ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

July 6, 2022

RESEARCH SECURITY: A NEW FRONTIER

Elisabeth Braw | American Enterprise Institute | Centre for Historical Analysis and Conflict Research
June 2022

Systemic exploitation of another country's science and technology innovation constitutes quintessential greyzone aggression as it strengthens the acting country, weakens the targeted country, and does so without it being clear where the bustle of globalization ends and the aggression begins. This report also proposes steps Western governments can take to curtail this practice. They include: establishment of a threshold above which the practice should be curtailed; national-security courses for STEM scientists and the tech start-up community; and more FIRRMA-style regulation of venture-capital funding. State-led exploitation of Western science and technology research, whether by China or any other country, poses a considerable risk to Western countries' competitive advantage in science and technology innovation — and thus to their economies. But unlike, say, gradual border alteration, exploitation of science and technology innovation is not straightforward greyzone aggression, because it is extremely difficult to pinpoint where legitimate cross-border scientific collaboration ends and systematic exploitation by one side of the other side's cutting-edge innovation begins.

Read the full article here.

DEEPFAKES AND STOLEN PII UTILIZED TO APPLY FOR REMOTE WORK POSITIONS

U.S. Department of Justice Federal Bureau of Investigation | June 28, 2022

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions. Deepfakes include a video, an image, or recording convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said. The remote work or work-from-home positions identified in these reports include information technology and computer programming, database, and software related job functions. Notably, some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information. Complaints report the use of voice spoofing, or potentially voice deepfakes, during online interviews of the potential applicants. In these interviews, the actions and lip movement of the person seen interviewed on-camera do not completely coordinate with the audio of the person speaking. At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually.

Read the full article here.

WHEN SHOULD U.S. RESEARCH BE STAMPED 'TOP SECRET'? NSF ASKS FOR A NEW LOOK AT THE ISSUE

Jeffrey Mervis | Science | June 30, 2022

The U.S. academic community is gearing up for a new effort to convince national policymakers that the benefits of keeping government-funded basic research out in the open—and not stamping it classified—far outweigh any threat to national security from sharing scientific findings. The National Science Foundation (NSF) has asked the National Academies of Sciences, Engineering, and Medicine (NASEM) to hold a workshop on factors affecting the classification of federally funded research. Tentatively scheduled for the fall, the meeting is expected to revisit a Cold War-era policy that sets openness as the gold standard and says any classification of fundamental research should be kept to a minimum. "Openness is axiomatic for scientists. But its value has not been articulated in a convincing way to the outside community," says John Mester, CEO of the Universities Research Association, a consortium that runs several government laboratories and research facilities.

Read the full article here.

EXPORT CONTROLS 'MATTER MORE THAN EVER,' US COMMERCE CHIEF RAIMONDO SAYS

Eric Martin | Bloomberg | June 29, 2022

US restrictions on exports "are at the red-hot center of how we best protect our democracies" because they cut off supply of crucial technologies tocountries that threaten American national security, Commerce Secretary Gina Raimondo said. Export controls "matter more than ever," she said at a conference hosted by the Commerce Department's Bureau of Industry and Security Wednesday, giving the example of restrictions on exports to Russia that may force the nation to ground as much as two-thirds of its commercial aircraft in the next four years to cannibalize them for spare parts. US shipments of all goods to the nation that invaded Ukraine have plunged about 95% by value, while American sales in the aviation and aerospace industry have tumbled 99.9%, Alan Estevez, under secretary of Commerce for Industry and Security, said earlier this month. Export controls by the US and 37 other nations are working, Raimondo said, adding "we have to do it over a sustained period of time because, unfortunately, I don't think this is going to end anytime soon." The BIS spent months prior to Russia's invasion in late February coordinating potential export controls with global allies to make sure that Moscow wouldn't simply substitute technology exports from another nation for those that were blocked by the US.

Read the full article here.

CHINA LURED GRADUATE JOBSEEKERS INTO DIGITAL ESPIONAGE

Riya Ghosh | TechStory | July 2, 2022

The graduates of Chinese University have been bagged to pursue a job at a mysterious tech firm. The firm concealed the real description of the work which aimed at examining Western objectives for snooping and interpreting hacked data in relation to Beijing's commercial-scale findings system. When looked into the matter by a news agency, found and approached around 140 people working as a translator in the firm out of which maximum are government universities graduates in the English language. The students said that they acknowledged to employment commercials at Hainan Xiadun, a Chinese firm situated on the tropical southern island of Hainan. The recruitment procedure comprised interpretation assessments on sensitive papers accessed from the United States government offices and directions to examine people at Johns Hopkins University, a major intelligence aim. The company has been accused by a United States court in 2021 of being espionage for the APT40 hacking association of China.

Read the full article here.

REPAIR THE DAMAGE DONE BY DOJ WRONGLY TARGETING CHINESE SCIENTISTS

Steven A. Kivelson and Peter F. Michelson | The Hill | June 29, 2022

The Department of Justice's "China Initiative" — now formally canceled – was a wrong-headed response to a real issue. To begin repairing the damage done, the United States government and U.S. research universities should actively promote open scientific collaboration with scientists and students in and from China, and from around the world. This is essential not only to justify our self-image as the land of opportunity, but also because U.S. international leadership in science and technology relies on these talented immigrants. The initiative ostensibly aimed to protect U.S. businesses and laboratories from intellectual property theft and economic espionage, but it was heavily criticized for possible racial profiling and anti-Asian and Chinese bias. Theft of information essential to our national security is very much on the minds of U.S. legislators and the executive branch. Some countries — China and Russia being examples — do not adhere to the codes of conduct that we espouse. (As an aside, one can wonder whether our country is as deferential to the dictates of international law as we should be.)

Read the full article here.

NIST ANNOUNCES FIRST FOUR QUANTUM-RESISTANT CRYPTOGRAPHIC ALGORITHMS

Chad Boutin | National Institute of Standards and Technology | July 5, 2022

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has chosen the first group of encryption tools that are designed to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on every day — such as online banking and email software. The four selected encryption algorithms will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years. "Today's announcement is an important milestone in securing our sensitive data against the possibility of future cyberattacks from quantum computers," said Secretary of Commerce Gina M. Raimondo. "Thanks to NIST's expertise and commitment to cutting-edge technology, we are able to take the necessary steps to secure electronic information so U.S. businesses can continue innovating while maintaining the trust and confidence of their customers."

Read the full article here.

CHINA ACCUSES NSA OF FOXACID HACK ATTACK ON SCIENCE RESEARCH GROUPS

Zhang Tong | South China Morning Post | July 2, 2022

China's research institutes have come under a cyberattack launched by the US government, according to China's cybersecurity authorities. The National Computer Virus Emergency Response Centre in Beijing said on Wednesday that FoxAcid, a hacking program linked to the US National Security Agency (NSA), was found in hundreds of key information systems used by scientific research institutes. The centre said the attack could signal NSA preparations for larger-scale cyberwarfare. "We encourage all users from all over the world to be aware of the risk and the fact that Chinese research institutions were not the only victims," the centre said. "Government, academic, and business bodies around the world might all become targets of the NSA. "When running a new 'colour revolution' operation, such a weapon enables US intelligence agencies to steal sensitive data at any time, and cause outages of critical infrastructure in wartime." FoxAcid first came to public attention in 2013, with the revelations of former NSA contractor Edward Snowden.

Read the full article here.

NEAR-UNDETECTABLE MALWARE LINKED TO RUSSIA'S COZY BEAR

Simon Sharwood | The Register | July 6, 2022

Palo Alto Networks' Unit 42 threat intelligence team has claimed that a piece of malware that 56 antivirus products were unable to detect is evidence that state-backed attackers have found new ways to go about the evil business. Unit 42's analysts assert that the malware was spotted in May 2022 and contains a malicious payload that suggests it was created using a tool called Brute Ratel (BRC4). On its rather brazen website, BRC4 is described as "A Customized Command and Control Center for Red Team and Adversary Simulation". The tool's authors even claim they reverse-engineered antivirus software to make BRC4 harder to detect. The malware Unit 42 observed starts life as a file that pretends to be the curriculum vitae of a chap named Roshan Bandara. Unusually, Bandara's CV is offered as an ISO file – a disk image file format.

Read the full article here.

THE CRYPTOPOCALYPSE IS NIGH! NIST ROLLS OUT NEW ENCRYPTION STANDARDS TO PREPARE

Dan Goodin | Ars Technica | July 5, 2022

In the not-too-distant future—as little as a decade, perhaps, nobody knows exactly how long—the cryptography protecting your bank transactions, chat messages, and medical records from prying eyes is going to break spectacularly with the advent of quantum computing. On Tuesday, a US government agency named four replacement encryption schemes to head off this cryptopocalypse. Some of the most widely used public-key encryption systems—including those using the RSA, Diffie-Hellman, and elliptic curve Diffie-Hellman algorithms—rely on mathematics to protect sensitive data. These mathematical problems include (1) factoring a key's large composite number (usually denoted as N) to derive its two factors (usually denoted as P and Q) and (2) computing the discrete logarithm that key is based on. The security of these cryptosystems depends entirely on how difficult it is for classical computers to solve these problems.

Read the full article here.

SCIENCE AND SECURITY: SETTING THE DIRECTION FOR THE UK'S RESEARCH RELATIONSHIP WITH CHINA

Peter Carlyon | RAND Corporation | June 30, 2022

The United Kingdom's relationship with China has undergone remarkable transformation in recent times. After enjoying a mutually proclaimed 'golden era' of collaboration throughout the 2010s, concerns over China's ambitions and its threat to UK security have infused the bond between the two nations with suspicion. The idea of decoupling from China, at least in certain aspects, has been raised frequently in the early 2020s—most recently following Russia's invasion of Ukraine, which prompted Liz Truss to announce to China in April 2022 that 'we have shown with Russia the kind of choices we're prepared to make when international rules are violated.' One form of UK-China cooperation which is particularly fraught is academic collaboration.

Read the full article here.