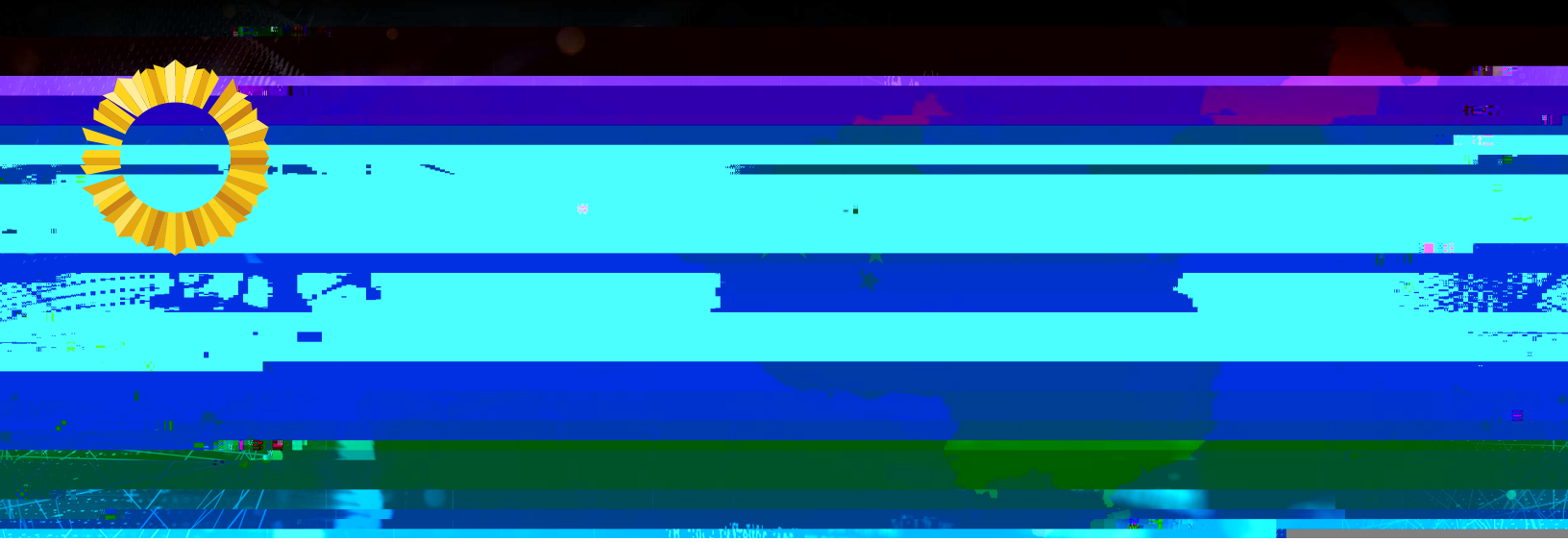

plagiarism in 2008, its analysis of articles published over a two-year period found approximately 31% of papers exhibited "unreasonable" copying and plagiarism, according to the journal director.

Second, the Chinese government has historically sponsored economic espionage, and China is the world's principal infringer of intellectual property. The annual cost to the U.S. economy of counterfeit goods, pirated software, and theft of trade secrets is between $225 billion and $600 billion.

Lastly, while the vast majority of students and researchers from China are in the United States for legitimate academic reasons and contribute to the diversity of backgrounds and ideas important in our society, the Chinese government uses some Chinese students—mostly post-graduate students and post-doctorate researchers studying science, technology, engineering, and mathematics (STEM)—and professors to operate as non-traditional collectors of intellectual property. These Chinese scholars may serve as collectors—wittingly or unwittingly—of economic, scientific, and technological intelligence from U.S. institutions to ultimately benefit Chinese academic institutions and businesses.

Regardless of motive, this exploitation comes at great cost to U.S. interests. When these foreign academics unfairly take advantage of the U.S. academic environment, they do so at a cost to the institutions that host them, as well as to the greater U.S. innovation ecosystem in which they play a role. Directly or indirectly, their actions cost money, jobs, expertise, sensitive information, advanced technology, first-mover advantage, and domestic incentive to innovate.

The FBI values academic integrity and rules-based scholarship, and we recognize international academics infuse campuses—and greater U.S. society—with a diversity of ideas that helps fuel the continued growth of the U.S. economy. According to the current numbers, immigrants—including many who first came to America as international stu-

HE CHINE E GO ERNMEN E A HOLE OF OCIE Y APPROACH O AD ANCE I ECONOMIC DE ELOPMEN ACHIE E GENERA IONAL AD ANCE IN RE EARCH AND DE ELOPMEN AND A E MONEY YO R NI ER I Y OR IN I ION PROFE OR DEN OR RE EARCH MIGH BE ARGE ED

CASE EXAMPLE

An American aerospace engineering professor at a Michigan university accepted a Chinese student's request to study with him. The student indicated she was a□liated with a Chinese civilian institution and expressed an interest in the professor's work. However, her China-based address in the university directory corresponded to a college for Chinese military o□cers, and she had previously published an article about improving China's anti-satellite technology. According to the professor, the Chinese student pressured him to reveal secrets about his work and was likely interested in research with military satellite applications.

This case describes how foreign adversaries like China sometimes task students to hide connections to a foreign government—in this case, a foreign military. To combat theft of technology and research, colleges and universities should consider proactive steps to ensure students and faculty understand how to protect intellectual property e□ectively, how to share and protect information responsibly, and how to avoid potential threats or compromises before they arise. Universities, as stewards of taxpayer research dollars, should consider implementing and enforcing clearer—and, in some cases, more restrictive—guidelines regarding funding use, lab access, collaboration policy, foreign government partnership, nondisclosure agreements, and patent applications. Additionally, the more willing colleges and universities are to engage with U.S. law enforcement as issues arise and suspicious circumstances become noticed, the more likely it is that the FBI and its partners can help to mitigate risk or minimize damage to these colleges and universities.

act cs Fore gn Adversar es se to arget Acade a

Foreign adversaries leverage joint research opportunities, language and cultural training, unsolicited invitations, visiting students and professors, and state-sponsored industrial and technical espionage to support their military and commercial research, development, and acquisition.

The tactics below all represent legitimate opportunities for your university or institution. However, foreign adversaries might use any combination of them to strategically target you and your work.

ALEN RECR I MEN OR BRAIN GAIN PROGRAM encourage the transfer of original ideas and intellectual property from U.S. universities. For example, China's talent recruitment plans, such as the Thousand Talents Program, o□er competitive salaries, state-of-the-art research facilities, and honorific titles, luring both Chinese overseas talent and foreign experts alike to bring their knowledge and experience (or that of advisors and colleagues) to China.

Association with talent recruitment plans by itself is not illegal; however, potential participants and their employers should be aware of legal issues that may arise as a result of participation, including violation of export-control laws, economic espionage, or violation of employer conflict-of-interest policies. A simple download of intellectual property or proprietary information has the potential to become criminal activity.

FOREIGN DEN OR I I ING PROFE OR are usually studying or working at U.S. universities for legitimate reasons. However, some foreign governments coerce legitimate students into reporting on the research they are doing in the Unites States—or even o□er scholarships or funding in exchange for the information.

LANG AGE AND C L RAL RAINING opportunities can enable foreign adversaries to use universities not only to increase their understanding of the local language and culture, but also to make contacts.

F NDING AND DONA ION provided by foreign adversaries can enable universities to establish cultural centers, support academic programs, or facilitate joint research while also fostering goodwill and trust between the donor organization and university. However, a foreign adversarial funding organization could place stipulations on how the programs or centers function or install its own recruits in positions with little or no university oversight.

ELICI A ION of information about your research or work can come in many forms. A foreign adversary might try to elicit information by using flattery, assuming knowledge, asking leading questions, claiming a mutual interest, or feigning ignorance.

JOIN RE E

CASE EXAMPLE

CASE EXAMPLE

A Chinese-American employee at a U.S. university established an internship placement service for American students interested in traveling to China for student exchanges. However, the employee was also knowingly in contact with a Chinese intelligence o□cer who targeted American students for intelligence exploitation. The employee provided the intelligence o□cer with personal and identifying information about American graduate students in China, including their travel logistics, contacts, and studies. The following year, the employee provided the Chinese intelligence o□cer with email communications between the U.S. university and a U.S. company that managed international education

Deve op a ecur ty trategy

Ensure you have a security strategy to protect your institution's information and employees from potential physical and cyber threats. To develop this strategy, identify your most important research and assets and ensure you devote appropriate resources to their protection. Establish formal agreements and procedures to determine ownership of intellectual property.

Develop a prevention, recognition, and response plan tailored to addressing insider, foreign adversary, and cyber threats. Form teams made up of legal counsel, cyber experts, physical security specialists, and academic supervisors to specifically combat insider threats. Ensure your university or institution's response policies can be easily accessed by employees and that they adequately account for privacy and confidentiality.

Talk to your local FBI field o□ce to report any suspicious activities, request training, or ask for threat and awareness materials to ensure you remain up to date on evolving threats.

Co bat ng Fore gn Adversar es act cs to arget Your n vers ty or Inst tut on

ACADEMIC COLLABORA ION is necessary to advance knowledge. Simple security measures, however, can go a long way in preventing the loss of current research and future opportunities. Consider the hidden risk of unsolicited o□ers for employment, research collaboration, or conference attendance.

FOREIGNER I I can present potential vulnerabilities to sensitive university facilities. Keep visitor groups together and monitor them at all times during the duration of their visit to areas containing sensitive technology, products, or personal information. When possible, ensure all visitors have proper clearance and background checks before they enter your facilities. Be aware of last-minute additions to visitor lists, as foreign adversaries sometimes add individuals at the last minute in an attempt to steal your information. Prevent unauthorized access to computer systems and ensure visitors do not record building security access procedures by ensuring visitors do not take videos or photographs or plug portable media devices into university computers.

MALICIO CYBER AC I I Y can also present potential vulnerabilities. Monitor logs on these systems to better identify this activity:

- Firewalls
- Proxy
- Web Server
- Anti-virus
- Active directory
- Network Address Translation (NAT)
- Windows event
- Intrusion Detection System (IDS)
- Domain Name Server (DNS)

If you suspect a cyber intrusion, assess the nature and scope of the incident by isolating the a□ected systems, target, and origin of the activity. Collect the network logs and records. Implement your company's cyber response plan and report the incident to law enforcement.

\ hen n Doubt Report the Inc dent

When in doubt, report a security violation or cyber intrusion to your institution's security o□cer or your local FBI o□ce. *Do not* alert the person under suspicion. Your security o□cers or law enforcement partners will handle the interaction according to their response policies.

Although your first inclination might be to distance your university or institution from a harmful threat, terminate an employee, or expel a student, there is significant value in reporting a security violation or cyber intrusion to law enforcement. Monitoring and investigating the threat could uncover third party actors and reveal previously unknown vulnerabilities of your university or institution.

AY YO CAN PRO EC YO R ORGANIZA ION There are steps organizations may take to identify and deter potential threats. The FBI o□ers these for information, but each organization must assess applicability in terms of its own policies, processes, and legal guidelines.	NON□ TRADITIONAL COLLECTORS*	INSIDER THREATS	JOINT VENTURES	FRONT COMPANIES	CYBER
Conduct exit interviews to identify potential high-risk employees (such as terminated employees and retired employees with insider threat indicators)	●	●		●	
Create a program that regularly screens employees for insider threats	●	●	●	●	
Develop strong risk management and compliance programs			●	●	
Educate and regularly train employees on security policies and protocols	●	●	●	●	
Employ appropriate screening processes to hire new employees	●		●	●	●
Encourage responsible use of social media sites and ensure online profiles have proper security protections in place					●
Ensure the company in question has been vetted through diligent research			●	●	
Ensure physical security personnel and information technology security personnel have the tools they need to share information	●	●	●		●
Ensure proprietary information is carefully protected	●	●	●	●	●
Ensure retired, separated, or dismissed employees turn in all company-issued property	●	●			●
Establish Virtual Private Networks (VPNs) for added protection					●
Evaluate the use of nondisclosure agreements and policies restricting the removal of company property	●	●		●	
Install Intrusion Detection Systems (IDSs)					●
Monitor computer networks routinely for suspicious activities	●	●	●		
Negotiate joint venture terms and penalize actions that contradict the agreement			●		
Provide nonthreatening, convenient methods for employees to report suspicious behavior, and encourage such reporting	●		●	●	●
Provide security personnel with full access to human resources data	●	●		●	
Routinely monitor computer networks for suspicious activities	●	●		●	●
Update software, firewalls, and anti-virus programs					●

**A non-traditional collector is an individual who is not operating on behalf of an intelligence service but who collects information from the United States and other foreign entities to support foreign government–directed objectives.*

For More Information

ra n ng Mater a s		
ORGANIZA ION	CON AC	DE AIL
Center for Development of Security Excellence		