FEDERAL BUREAU OF INVESTIGATION

CHINA: THE RISK TO ACADEMIA

As of March 2018, more than 1.4 million international students and professors were participating in America's open and collaborative academic environment. The inclusion of these international scholars at U.S. colleges and universities entails both substantial benefit—and notable risk. Many of these visitors contribute to the impressive successes and achievements enjoyed by these institutions, which produce advanced research, cutting-edge technology, and insightful scholarship. However, this open environment also puts academia at risk for exploitation by foreign actors who do not follow our rules or share our values.

The annual cost to the U.S. economy of counterfeit goods, pirated software, and theft of trade secrets is

$225–$600 BILLION

The vast majority of the 1.4 million international scholars on U.S. campuses pose no threat to their host institutions, fellow classmates, or research fields. On the contrary, these international visitors represent valuable contributors to their campuses' achievements, providing financial benefits, diversity of ideas, sought expertise, and opportunities for cross-cultural exchange. Any research institution hoping to be—and to remain—among the best in the world must attract and retain the best people in the world, wherever they are from. The FBI recognizes, and values, this unique package of benefits these international students and professors provide.

However, some foreign actors, particularly foreign state adversaries, seek to illicitly or illegitimately acquire U.S. academic research and information to advance their scientific, economic, and military development goals. By doing so, they can save their countries significant time, money, and resources while achieving generational advances in technology. Through their exploitative efforts, they reduce U.S. competitiveness and deprive victimized parties of revenue and credit for their work. Foreign adversaries' acquisition efforts can come in many forms, including overt theft, plagiarism, elicitation, and the commercialization of early-stage collaborative research.

As foreign adversaries use increasingly sophisticated and creative methodologies to exploit America's free and open education environment, the United States faces an ever-greater challenge to strike a sustainable balance between unrestricted sharing and sufficient security within this education ecosystem. Through a whole-of-society approach that includes increased public awareness, academic vigilance, industry self-protection, government and law enforcement collaboration, and legislative support, the U.S. higher education system can continue to enjoy the manifold contributions that international academics provide, while minimizing the risk they (and their affiliated home governments) pose to U.S. security priorities. The FBI maintains that striking this balance is possible and necessary.

Foreign adversaries exploit America's deeply held and vital culture of collaboration and openness on university campuses, with the Chinese government posing a particular threat to U.S. academia for a variety of reasons. First, it does not play by the same rules of academic integrity that U.S. educational institutions observe. Many recent high-profile examples show plagiarism is commonplace throughout Chinese academic and research institutions. Illustrative of this endemic plagiarism, when the *Journal of Zhejiang University–Science* became the first in China to employ text analysis software to identify

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 students—founded almost a quarter of all new U.S. businesses, nearly one-third of our venture-backed companies, and half of Silicon Valley's high-tech startups. More than 18% of Fortune 500 companies were founded by immigrants.

Academic environments represent the very bedrock on which this country is built and upon which its future depends. These campuses are where young minds from diverse background and countries discover new technologies, learn novel concepts, establish crucial connections, pursue innovation, and lay the groundwork for America's continued leadership in scholarship and technology advancement for decades to come. If these open, free, and collaborative environments are compromised, limited, or obstructed, all of us here today—and the country's future generations—lose. We want to work with you to address these challenges.

DIFFERENCES IN BUSINESS PRACTICES	
UNITED STATES	**CHINA**
Generally accessible market	Highly restrictive market
Market economy	State-run economy
Development by innovation	Development by theft, replication, and commercialization
Independent judiciary and separation of powers	Judiciary subordinate to the government
Laws protecting intellectual property	Unequal protection of intellectual property
No government-sponsored economic espionage	Government-sponsored economic espionage

CHINA'S DEVELOPMENT STRATEGY

The Chinese government's strategic goals include becoming a comprehensive national power, creating innovation-driven economic growth, and modernizing its military. It aspires to equal or surpass the United States as a global superpower and influence the world with a value system shaped by undemocratic, totalitarian ideals. Using a whole-of-society approach to achieve these goals, the Chinese government takes advantage of every opportunity—from academic collaboration to economic espionage—to develop and maintain a strategic economic edge.

To achieve its economic, technological, and military goals, the Chinese government relies on various state-directed plans. These plans provide insight into the kinds of knowledge, research, intellectual property, and trade secrets the country targets and seeks to acquire from foreign sources. At present, China's government has as many as 100 plans guiding China's foreign acquisition, and their scale and influence are impressive. Two of the most important among these plans include the 13th Five-Year Plan and the Made in China 2025 Plan, both of which help to guide the country's overall strategic direction.

The Made in China 2025 Plan lists 10 domestic Chinese industries from which the government of China seeks to eliminate any foreign-produced technology:

- Information technology
- Computer numerical control machine tools and robotics
- Aerospace equipment
- Marine engineering equipment and high-tech ships
- Advanced rail transportation equipment
- Energy-efficient and new-energy automobiles
- Electric power equipment
- Agricultural equipment
- New materials
- Biomedicine and high-performance medical instruments

ACCORDING TO THE CHINESE GOVERNMENT'S STATE COUNCIL, CHINA USES THE FOLLOWING FOUR-STEP DEVELOPMENT PROCESS TO GAIN A TECHNOLOGICAL EDGE:

1 INTRODUCE	The Chinese government uses numerous methods—some legitimate but others, such as stealing technology from foreign competitors, meant to illicitly **introduce** foreign technology and knowledge to China.
2 UNDERSTAND	The Chinese government uses its numerous civilian and military institutions and resources to **understand** the materials acquired from foreign sources.
3 ASSIMILATE	Those same institutions **assimilate** foreign technology and knowledge into Chinese infrastructure—frequently by reverse-engineering it.
4 RE-INNOVATE	Chinese institutions **re-innovate** foreign technologies, such as military aircraft, high-speed trains, and nuclear reactors, to develop new and state-of-the-art technology. Such advances allow China to achieve generational advances and save time and money on research and development.

FOREIGN TRADECRAFT USED AGAINST ACADEMIA

Academic Targets of Foreign Adversaries

If your university or institution's research has technical applications, expect foreign adversaries to target it. If your university or institution invests significantly in expensive research and development, anticipate foreign adversaries will target it—including those conducting the research and the development processes you use to produce your end products. Some of the information these adversaries target might seem insignificant, but by bypassing the research and development phase and stealing your technical information or products, foreign adversaries can gain a competitive economic and military advantage.

Research can lead to the development of products with national security applications. Even if the technologies and their applications are not currently classified, they could be in the future. Foreign adversaries know this and seek to obtain this technology when it is least restricted and easiest to obtain: before it is classified.

Foreign adversaries might target your:

- Students, professors, and researchers with access to research and technical information (particularly graduate and post-doctorate students)
- Pre-publication research results
- Research data
- Techniques and processes
- Laboratory equipment and software
- Pre-classification research
- Access protocols
- Budget estimates and expenditures
- Computer access protocols
- Computer network design
- Customer and employee data
- Equipment specifications
- Passwords for your computer, phone, or accounts
- Phone and property data
- Proprietary research, formulas, and processes
- Prototypes or blueprints
- Software, including source codes
- Technical components and plans
- Vendor information and supply chain
- Confidential documents
- Grant data

CASE EXAMPLE

A Chinese researcher at a Midwestern medical school was charged with economic espionage for illegally acquiring an American researcher's patented cancer research and transferring it to a university in China. The American researcher placed several containers of a patented cancer research compound on his desk, stepped away, and found them gone when he returned. The university's review of security surveillance footage showed the Chinese researcher was the only other individual who had entered the American researcher's office that day. The Chinese researcher had also accessed the university's computer server and attempted to delete proprietary information related to the research and compound. When questioned by law enforcement, the Chinese researcher indicated he could not understand English, despite his coworkers' assurances he spoke the language well and had lived in the United States for several years. He was arrested only days before he was scheduled to fly to China and ultimately pleaded guilty to intentionally accessing a computer without authorization and obtaining information worth more than $5,000.

This case highlights the vulnerability even protected, patented materials and information face due to the open, collaborative environment of U.S. academic institutions, further emphasizing the need for constant vigilance and proactive protection. This case also highlights the tremendous incentives foreign governments such as China are offering to their citizens to produce or procure (by whatever means necessary) cutting-edge research and technology through research funding and talent recruitment efforts.

THE CHINESE GOVERNMENT USES A WHOLE-OF-SOCIETY APPROACH TO ADVANCE ITS ECONOMIC DEVELOPMENT, ACHIEVE GENERATIONAL ADVANCES IN RESEARCH AND DEVELOPMENT, AND SAVE MONEY. YOUR UNIVERSITY OR INSTITUTION'S PROFESSORS, STUDENTS, OR RESEARCH MIGHT BE TARGETED.

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 affiliated 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 officers, 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 effectively, 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.

Tactics Foreign Adversaries Use to Target U.S. Academia

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.

TALENT RECRUITMENT OR "BRAIN GAIN" PROGRAMS 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, offer 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 STUDENTS OR VISITING PROFESSORS 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 offer scholarships or funding in exchange for the information.

LANGUAGE AND CULTURAL TRAINING 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.

FUNDING AND DONATIONS 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.

ELICITATION 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.

JOINT RESEARCH OPPORTUNITIES and collaborative environments, such as incubators or joint research centers, can enable a foreign adversary to obtain your research. They can also provide an opportunity to spot, assess, and befriend fellow STEM students or researchers who might assist—either wittingly or unwittingly—in passing your research and development to a foreign adversary.

FOREIGN TRAVEL can leave American students, professors, and researchers vulnerable to targeting through searches of luggage and hotel rooms, extensive questioning, manufacture of compromising situations, and confiscation of electronics. Foreign governments do not operate under the same laws or observe the same privacy rights that the U.S. government observes.

FOREIGN VISITORS entering sensitive research areas can pose a security risk to your intellectual property or competitive edge. Some visitors might verbally elicit information, some might brazenly ignore the security parameters of a tour, and others might use concealed electronic devices to obtain restricted information or access.

CASE EXAMPLE

A well-known U.S. professor obtained a U.S. Air Force–funded contract to develop specialized plasma technology to control the flight of military drone aircraft. The professor inappropriately allowed two international students to work with him on the government-backed research and permitted the foreign nationals to access restricted, export-controlled data and equipment. The professor also illegally traveled to China with a laptop containing export-controlled research data—even though his university had counseled that the data must remain in the United States. The U.S. professor was convicted of conspiracy, wire fraud, and 15 counts of exporting defense articles and services without a license.

This example illustrates how universities can protect theft of technology from foreign adversaries by implementing and enforcing clear—and in some cases more restrictive—guidelines regarding funding use, lab access, collaboration policy, foreign government partnership, and nondisclosure agreements.

CASE EXAMPLE

A Chinese professor at a U.S. university contributed to a classified U.S. Department of Defense project. He was also a member of the Thousand Talents Program and an advisor for the Chinese government's Institute of Electronics and Automation Engineering at a Chinese university—as well as the lead scientist for an advanced technology project at a major Chinese research institute. The Chinese professor provided the Chinese institute with research that closely resembled the classified work he had performed for the U.S. Department of Defense.

This example shows the threat posed by programs like the Thousand Talents Program. Intentional or not, foreign governments' talent recruitment and "brain gain" programs encourage theft of intellectual property from U.S. universities. China's talent recruitment plans, such as the Thousand Talents Program, offer 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 at the expense of the United States.

Spotting Students or Professors

Foreign intelligence services routinely collect information about U.S. universities' programs, administrators, professors, and demographics. Foreign adversaries might target students and researchers with current or future access to sensitive information, including studying their motivations, weaknesses, politics, ambitions, and previous work. They can spend years targeting an individual and developing a relationship that leads the student, professor, or researcher—either wittingly or unwittingly—to provide information to the foreign adversary.

Foreign adversaries are particularly interested in American students or researchers traveling overseas who are sponsored by the U.S. government; conducting research with future, potentially classified applications; or seeking future U.S. government employment.

Foreign adversaries might use any of these techniques to access information or research via students, professors, or researchers:

- Appeals to ethnicity or nationality (for example, common ethnic heritage or dual-citizenship)
- Sponsorship of foreign travel
- Coercion
- Study abroad opportunities
- Overseas professional opportunities
- Talent recruitment programs
- Social engineering
- Scholarships or research funding
- Publishing opportunities
- Joint research opportunities

CASE EXAMPLE

American citizen Glenn Duffie Shriver was an undergraduate studying in Shanghai when he responded to an ad in a Chinese newspaper soliciting essays on U.S.-China relations. Shriver's essay submission led to interactions with three Chinese intelligence officers who represented themselves as municipal government officials. They developed a relationship with Shriver over time and eventually asked him to return to the United States and obtain employment with the U.S. government. After graduating, Shriver spent the next five years attempting to gain employment with the U.S. Department of State and the Central Intelligence Agency (CIA), all the while maintaining contact with the intelligence officers and accepting $70,000 from them. Shriver knew the purpose of his intended U.S. government employment was to gain access to national defense information and provide it to the Chinese government. While he was being processed for employment with the CIA, Shriver made false statements to conceal his relationship with the Chinese intelligence officers. He was arrested in 2010 and subsequently pleaded guilty to conspiracy to provide national defense information to a person not entitled to receive it. The following year, he was sentenced to four years in prison. The FBI's short film *Game of Pawns: The Glenn Duffie Shriver Story* is based on these events. Accessible at www.fbi.gov, the film educates viewers about the foreign intelligence threat Americans face abroad.

This example shows that foreign intelligence services seek to identify U.S. students who can help them gain access to information or persons of interest—either immediately or in the future. Foreign intelligence services develop initial relationships with U.S. students overseas under seemingly innocuous pretexts, such as job or internship opportunities, paid paper writing engagements, language exchanges, and cultural immersion programs. As these relationships develop, foreign intelligence services ask the U.S. students to perform tasks and provide information (which is not necessarily sensitive or classified) in exchange for payment or other rewards, slowly increasing their demands over time. Without proper awareness about this threat, U.S. students overseas have inadvertently become involved in espionage activities and have been prosecuted for these activities.

Insider Threats

Your university or institution may be vulnerable to damage from an insider—someone who has legitimate or illegitimate access to your information or research and provides that information to a foreign adversary. Insider threats could begin as early as the application phase, when applicants might be directed by foreign governments to seek enrollment in, or employment with, universities or research institutions with access to desired programs and persons.

Some of these behaviors might indicate an individual potentially poses an insider threat to your university or institution:

- Displays suitability issues, such as alcohol or drug abuse
- Insists on working in private
- Volunteers to help on classified or sensitive work
- Expresses an interest in covert activity
- Has unexplained or prolonged absences
- Rummages through offices or desks of others
- Misuses computer or information systems
- Attempts a computer network intrusion
- Has criminal contacts or associates
- Employs elicitation techniques
- Displays unexplained affluence
- Fails to report overseas travel, if required
- Takes classified or sensitive material home without authorization
- Conceals foreign contacts
- Lacks concern for or violates security protocols
- Brings audio or visual recording devices into work areas without authorization
- Unnecessarily photocopies or downloads sensitive material
- Attempts to gain access without a need to know
- Shows unusual interest in information outside the scope of his or her role
- Takes short trips to foreign countries for unexplained reasons

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 officer who targeted American students for intelligence exploitation. The employee provided the intelligence officer 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 officer with email communications between the U.S. university and a U.S. company that managed international education programs in China. The employee then provided the Chinese intelligence officer with résumés, interview information, and personal data to facilitate the targeting of students at several U.S. universities.

This example shows that foreign intelligence services seek to identify U.S. students who can help them gain access to information or persons of interest—either immediately or in the future. Foreign intelligence services develop initial relationships with U.S. students overseas under seemingly innocuous pretexts, such as job or internship opportunities, paid paper writing engagements, language exchanges, and cultural immersion programs. As these relationships develop, foreign intelligence services ask the U.S. students to perform tasks and provide information (which is not necessarily sensitive or classified) in exchange for payment or other rewards, slowly increasing their demands over time. Without proper awareness about this threat, U.S. students overseas have inadvertently become involved in espionage activities and have been prosecuted for these activities.

Foreign adversaries look for opportunities to exploit individuals' vulnerabilities and motivations to gain access to your research and development. In the past, foreign adversaries have targeted the following vulnerabilities and situations when exploiting insiders:

- Ideology (such as divided loyalty to a country other than the United States)
- Professional or academic opportunities, such as conferences
- Greed or financial stress
- Ego or self-image
- Coercion or compromise
- Anger, revenge, or disaffection
- The need for adventure or thrills

Cyber Techniques

Foreign adversaries might conduct computer intrusions by writing or manipulating computer code to gain access to, or install unwanted software on, your network. To do so, they could employ a variety of techniques.

CLICK-BAITING is when an adversary conceals hyperlinks beneath legitimate clickable content (such as "Like" and "Share" buttons on social networking sites). Once clicked, the links cause a user to unknowingly perform unwanted actions, such as downloading malware or sending the user's ID to a third party.

PHISHING is when an adversary conceals a link or file containing malware in something like an email, text message, or social media message that looks like it is from a legitimate organization or person. If clicked, the link or file compromises the recipient's electronic device and/or associated account.

SOCIAL ENGINEERING is when an adversary tricks a user into divulging confidential or personal information that may be used for fraudulent purposes.

UNPATCHED SOFTWARE EXPLOITATION is when an adversary takes advantage of people or companies that do not update their software regularly to conduct malicious activity, such as computer exploitation or malware installation.

SOCIAL MEDIA EXPLOITATION is when an adversary uses social media networks to exploit a user's personal connections—including his or her profile, content, and interactions on social media websites—to spot and assess employees for potential recruitment.

CASE EXAMPLE

After the FBI alerted it to a cyberattack on its College of Engineering's network, a large northeastern state university enlisted a third-party expert to identify the nature of the attack and take appropriate action. The third-party investigation revealed the presence of two sophisticated, previously undetected threat actors and confirmed at least one of the two attacks emanated from a threat actor based in China with a history of targeting victims in aerospace, defense, and academia. Evidence linked the China-based actor directly to the compromise of usernames and passwords issued by the College of Engineering and accessed via its network. The third-party investigation also revealed the university's network had been compromised for at least two years.

The university president said in a letter to the university community, "As we have seen in the news over the past two years, well-funded and highly skilled cybercriminals have become brazen in their attacks on a wide range of businesses and government agencies, likely in search of sensitive information and intellectual property." On an average day, the university blocks more than 20 million cyberattacks from around the world.

HOW TO PROTECT YOUR UNIVERSITY OR INSTITUTION

Your organization could consider adopting some of these suggested measures to identify and combat potential insider threats. Depending on your company's specific needs, policies, processes, and legal guidelines, you should determine what security measures are necessary to sufficiently protect your company's most important assets.

- Educate and regularly train employees on security policies and protocols.
- Ensure proprietary information is carefully protected.
- Employ appropriate screening processes to hire new employees.
- Develop strong risk management and compliance programs.
- Provide convenient ways for employees to report suspicious behavior, and encourage such reporting.
- Monitor computer networks routinely for suspicious activities.
- Provide security personnel with full access to relevant human resources data.
- Ensure physical security personnel and information technology security personnel have sufficient threat detection software, countermeasure tools, and protective processes in place.
- Implement a continuous evaluation program to persistently screen onboard employees.
- Conduct in-depth background checks on potential partners for associations with state-sponsored entities.
- Ensure retired, separated, or dismissed employees turn in all company-issued property.
- Ensure sufficiency of existing nondisclosure agreement requirements and policies restricting the removal of company property.

It is every university and institution's responsibility to safeguard its information. The FBI actively partners with universities and institutions to support this effort, providing counterintelligence tools and awareness training to help your schools and scholars recognize suspicious behavior and better protect your facilities and information. The FBI can collaborate with U.S. universities or institutions on a wide variety of topics, including:

- Responsibly performing U.S. government-funded research
- Countering foreign intelligence services' attempts to recruit U.S. students and professors
- Safeguarding personal and sensitive information
- Employing best practices for domestic and overseas campus safety
- Employing effective cybersecurity measures

Develop a Security Strategy

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 office to report any suspicious activities, request training, or ask for threat and awareness materials to ensure you remain up to date on evolving threats.

Combating Foreign Adversaries' Tactics to Target Your University or Institution

ACADEMIC COLLABORATION 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 offers for employment, research collaboration, or conference attendance.

FOREIGNER VISITS 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.

MALICIOUS CYBER ACTIVITY can also present potential vulnerabilities. Monitor logs on these systems to better identify this activity:

- Firewalls
- Proxy
- Web sever
- 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 affected 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.

When in Doubt, Report the Incident

When in doubt, report a security violation or cyber intrusion to your institution's security officer or your local FBI office. *Do not* alert the person under suspicion. Your security officers 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.

WAYS YOU CAN PROTECT YOUR ORGANIZATION There are steps organizations may take to identify and deter potential threats. The FBI offers 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

Training Materials		
ORGANIZATION	**CONTACT**	**DETAILS**
Center for Development of Security Excellence	http://cdse.edu/catalog/elearning/INT101.html	*Insider Threat Awareness Course (INT101.16)*
Center for Development of Security Excellence	http://www.cdse.edu/toolkits/insider/index.php	*Insider Threat Toolkit*
Software Engineering Institute, Carnegie Mellon University	https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738	*Common Sense Guide to Mitigating Insider Threats, Fifth Edition*
Federal Bureau of Investigation	http://www.fbi.gov	Numerous publications and videos on the threat from foreign adversaries targeting U.S. businesses.

Additional Contacts	
ORGANIZATION	**CONTACT INFORMATION**
FBI Field Offices	https://www.fbi.gov/contact-us/field-offices
FBI Internet Crime Complaint Center	http://www.ic3.gov
National Cyber Investigative Joint Task Force	855.292.3937 | cywatch@fbi.gov
National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security	888.282.0870 | NCCIC@hq.dhs.gov

CONTACT US:

For more information, contact your local field office at *https://www.fbi.gov/contact-us/field-offices*