INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

MAY 2021

Insider Threats and Commercial Espionage: *Economic and National Security Impacts*

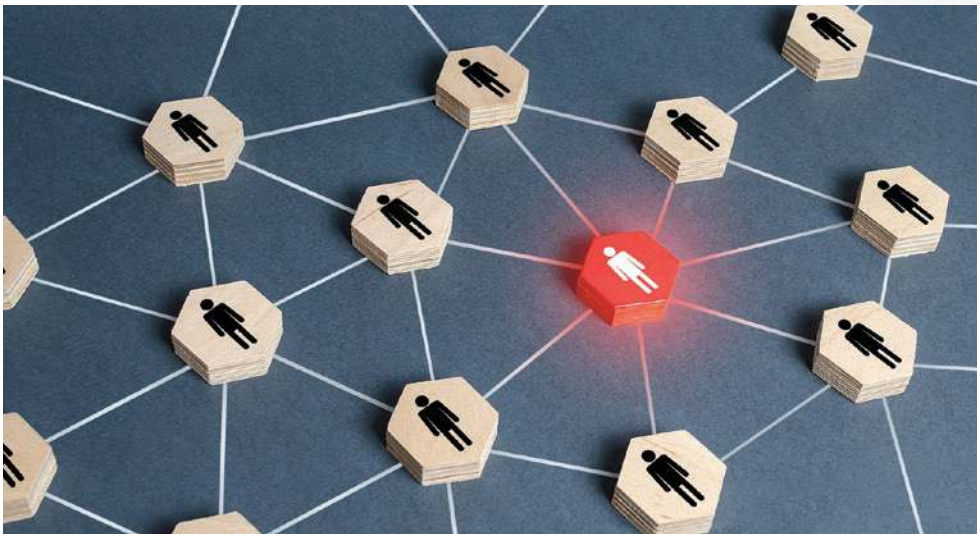
Presented by

INSA'S INSIDER THREAT SUBCOMMITTEE

Building a Stronger Intelligence Community

EXECUTIVE SUMMARY

Economic espionage causes significant harm to the American economy and to U.S. national security. The theft of intellectual property costs the United States between one and three percent of its $21 trillion annual GDP and enables foreign competitors to bring comparable products or technologies to market at a fraction of the cost and in far less time. Since many advanced technologies have military and intelligence applications, the theft of related information enables U.S. adversaries to enhance their capabilities and better counter those of the United States. China is the most aggressive actor behind the theft of commercial secrets, with 20 percent of U.S. companies claiming that entities tied to China have stolen their intellectual property.

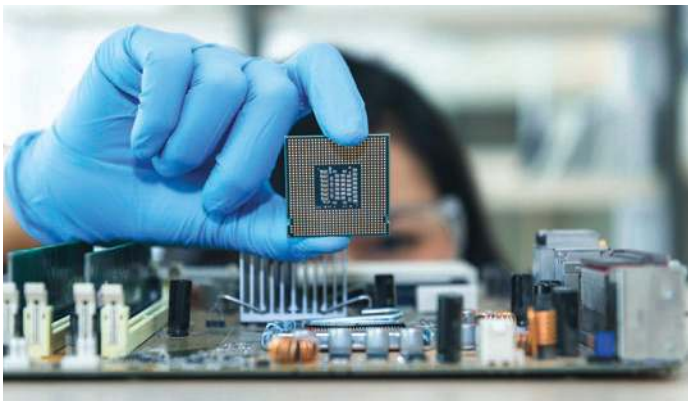


This paper will review the threat posed by economic espionage and highlight the role of trusted inside actors in stealing sensitive material for the benefit of foreign competitors. Through a better understanding of why trusted insiders choose to steal economic and commercial information, government officials and industry executives can develop strategies to mitigate and prevent economic espionage and its detrimental effects on the United States. Recommended steps include intensified efforts by companies and universities to instill a culture of security in their organizations; expanded government outreach to corporate and academic leaders, particularly at smaller institutions, regarding foreign adversaries' targets and methodologies; and government programs to help companies and universities—particularly ones that conduct government-sponsored research and development—evaluate their security postures and establish comprehensive insider threat programs.

INTRODUCTION

Economic espionage poses a serious threat to American businesses and to the overall prosperity of the United States.[1] The theft of intellectual property (IP), through both open and clandestine methods, can provide foreign entities with valuable proprietary commercial information at a fraction of the true cost of its research and development and in far less time than it would take to develop the information itself. Given that many advanced technologies have intelligence and military applications, the theft of related information also has significant implications for U.S. national security.

Valuable commercial information is often stolen by hacking into a network, though advanced cybersecurity tools create a formidable defense against remote electronic attacks. However, if an adversary can recruit an employee or trusted partner of the targeted organization, that person can use their access to provide documents and data—and critical context and know-how—while operating under the radar and evading detection. Trusted insiders can identify and work around physical and network security controls, particularly when their legitimate access to information can disguise their illegitimate intentions.



This paper will examine these *insider threat actors* in an attempt to understand why individuals choose to steal IP from an organization with which they are affiliated. A deeper understanding of what compels a trusted insider to commit IP theft will enable information and physical security professionals to develop effective safeguards and preemptive strategies to counter economic espionage.

“

A deeper understanding of what compels a trusted insider to commit IP theft will enable information and physical security professionals to develop effective safeguards and preemptive strategies to counter economic espionage.

BACKGROUND

Foreign economic and industrial espionage against the United States represents one of the most significant threats to America's prosperity, security, and competitive advantage, costing the United States between one and three percent[2] of its $21 trillion annual GDP.[3] The theft of intellectual property eviscerates the value of past investments to develop a marketable product or technology and undermines prospects for future revenues. Stolen IP enables competitors to sell nearly identical products with virtually no R&D costs and often undercut the American developer on price. While political and military espionage has long been treated as a threat to national security, it is only in the past few decades that the theft of commercial trade secrets has been recognized as a problem of national import. In 1996, Congress enacted The Economic Espionage Act (EEA),[4] which made the theft or misappropriation of IP and trade secrets a federal crime. The EEA criminalized economic and industrial espionage executed for the benefit of a foreign government, as well as the more common commercial theft of trade secrets, regardless of the beneficiary.[5] In February 2020, the Office of Director of National Intelligence (ODNI) issued a National Counterintelligence Strategy for the United States that focuses largely on the theft of U.S. intellectual property.[6]

Global Internet connectivity made it possible for adversaries to steal data from U.S. firms from the safety of their own territory. In 2011, the U.S. National Counterintelligence Executive (NCIX) highlighted cyber-enabled espionage capabilities as one of the most pervasive threats posed by foreign intelligence services to U.S. research, development, and manufacturing sectors.[7] In a 2018 report on Foreign Economic Espionage in Cyberspace, the National Counterintelligence and Security Center (NCSC), the successor to NCIX, wrote that cyberspace is the preferred attack vector for "a wide range of industrial espionage threat actors, from adversarial nation-states, to commercial enterprises operating under state influence, to sponsored activities conducted by proxy hacker groups."[8]

> Organizations must understand how to counter the unpredictable nature of their employees, contractors, and business partners. Government, industry, and academia must better understand the motivations that drive trusted employees with access to valuable information to reveal it to competitors or adversaries.

Despite the attention given to hacking and cyber-enabled espionage, humans remain at the center of the threat. According to Carnegie Mellon's Software Engineering Institute (SEI), employees, contractors, and business partners (i.e., insiders) with direct access to information, facilities, and systems "have a significant advantage over external attackers. They are not only aware of their organization's policies, procedures and technology; they are also familiar with its vulnerabilities (for example, this can include loosely enforced policies and exploitable flaws in networks)."[9] Carnegie Mellon's CERT Insider Threat Center concluded that insiders were suspected or known to be responsible for approximately 23 percent of electronic crimes, and 45 percent of respondents to a 2015 CERT survey believed insiders pose greater risks than outside attackers.[10]

Protecting networks from external cyber attack is therefore insufficient; organizations must understand how to counter the unpredictable nature of their employees, contractors, and business partners. Government, industry, and academia must better understand the motivations that drive trusted employees with access to valuable information to reveal it to competitors or adversaries.

THE THREAT OF ECONOMIC ESPIONAGE

Research and development (R&D) investments have fueled American innovation. U.S. government, industry, and academic institutions devoted $580 billion to R&D in 2018, representing more than a quarter of all R&D expenditures in the world.[11] Innovative technologies take significant amounts of funds and many years to develop—sunk costs that increase the price companies must charge for the technologies they eventually bring to market. If a competitor can steal critical research, it can reproduce the innovation at a fraction of the cost and in far less time, which enables it to undercut its price and thereby steal market share from the original developer.

Adversaries willing to recruit or take advantage of individuals with inside knowledge can gain extraordinary access to proprietary R&D information. They will work diligently to identify insiders who are susceptible to coercion or bribery; who may be ignorant of, or careless about, security policies; and who are in a position to abscond with trade secrets. Access to an insider enables an adversary to circumvent security controls from the inside rather than penetrate them from the outside.

> U.S. academic institutions, with their great concentration of creative talent, cutting edge research endeavors, and open engagement with the world of ideas, are an especially attractive environment for foreign collectors targeting America's R&D wealth.

FOREIGN THREATS

While Russia, Iran, North Korea, and other U.S. adversaries have tried to steal commercial information, China is by far the most aggressive actor targeting U.S. companies' intellectual property. Indeed, 20 percent of American companies claim that entities tied to China have stolen their intellectual property,[12] and more than half of EEA prosecutions involve a nexus to China. In congressional testimony in April 2021, FBI Director Christopher Wray stated that the FBI has more than 2,000 open investigations with links to the Chinese government and that it opens a new China-related espionage case every ten hours.[13]

China's "Made in China 2025" notice includes ten strategic advanced technology manufacturing industries that China aims to advance. These include next generation information technology, robotics and automated machine tools, maritime vessels and marine engineering equipment, electrical generation and transmission equipment, and biotechnology.[14] The U.S. Department of Justice's "China Initiative," launched in November 2018, seeks to counter Chinese national security threats by identifying and prosecuting cases related to Chinese thefts of U.S. intellectual property.[15] Among the dozens of cases pursued under the China Initiative are indictments of scientific researchers, engineers, professors, hackers, and businesspeople—both American and Chinese.[16]

- A Chinese-born U.S. Navy officer, his naturalized U.S. citizen spouse, and two Chinese nationals were indicted in November 2019 for fraudulently attempting to export inflatable boats with military applications to China.[17]
- In October of 2020, an American and a Chinese national were indicted for conspiring to steal technology from a Houston-area oil and gas manufacturer on behalf of two Chinese companies.[18]
- In November of 2020, a university rheumatology professor and researcher pleaded guilty to lying on grant applications and making false statements to federal authorities for planning to provide China with insights from research funded by the National Institutes of Health.[19]

China recruits U.S. scientists, engineers, and others to obtain critical technologies, expertise, and intellectual property through its Thousand Talents Program and more than 200 similar initiatives to surreptitiously acquire foreign technology. U.S. nationals recruited by the program provide proprietary data to Chinese counterpart institutions in exchange for payment, which they typically do not disclose to their full-time U.S. employers or funders.[20] Some participants, according to a U.S. Senate committee report, establish "shadow labs" in China to mirror the work they do in the United States, based on research data funded by their U.S. employers.[21]

- On January 13, 2021, Meyya Meyyappan, a senior NASA scientist, pleaded guilty to making false statements related to his participation with the Chinese Thousand Talents Program. Meyyappan held a trusted position at NASA as Chief Scientist for Exploration Technology at NASA's Ames Research Center in California.[22]
- In January of 2020, Charles Lieber, Chair of Harvard's Chemistry Department and one of the world's leading researchers in the field of nanotechnology, was arrested for sharing his research, in exchange for payment, with Wuhan University of Technology (WUT) through the Thousand Talents Program. U.S. government agencies, including the National Institute of Health and the Department of Defense, had provided Lieber with more than $15 million to fund his research in the United States.[23]
- In July of 2019, Kang Zhang, the Chief of Eye Genetics at the University of California San Diego Shiley Eye Institute and a participant of the Thousand Talents Program, resigned after it was revealed that he failed to disclose he was a primary shareholder of a publicly traded Chinese biotechnology company that specializes in the same work he performed at UCSD.[24]

RISKS OF ACADEMIA'S OPEN CULTURE

In academia, and particularly in scientific and medical research, scholars lean towards the noble goal of exchanging ideas to promote learning and progress to the benefit of all, regardless of heritage, national origin, race, creed, or religious views. This is, admittedly, necessary if we as a global society hope to continue to advance quality of life for generations to come.

Unfortunately, foreign adversaries can take advantage of this openness to the detriment of U.S. national and economic security. As former National Counterintelligence Executive Michelle van Cleave testified at a congressional hearing in April 2018, "U.S. academic institutions, with their great concentration of creative talent, cutting edge research endeavors, and open engagement with the world of ideas, are an especially attractive environment for foreign collectors targeting America's R&D wealth."[25]

In 2019, "national security agencies, federal granting agencies, the White House and members of Congress…all signaled their increasing concern…" about "theft of sensitive academic research by foreign competitors."[26] In many cases, the research being stolen was funded by U.S. taxpayers through institutions like the National Institutes of Health (NIH). An NIH outreach campaign encouraging administrators of government research grants to assess security risks resulted in more than 180 investigations of scientists at 71 institutions.[27]

The U.S. Government has taken significant steps towards curbing such threats, including securing sensitive studies, classifying some research, adding restrictions to visas in certain STEM fields, limiting Chinese graduate students in technological fields to one-year stays in the United States, and restricting participation "in foreign talent recruitment programs operated by countries deemed…'sensitive.'" [28]

DOMESTIC INDUSTRIAL ESPIONAGE

Domestic economic espionage, also known as industrial espionage or corporate espionage, can be just as damaging to American companies as foreign-based malicious activity. U.S. corporations face intense competition both at home and abroad, and while methods of spying on competitors have changed over time, the motivations to uncover a rival's trade secrets have persisted. Advances in technology make the protection of IP and sensitive data even more difficult to protect and more critical to a company's operations and economic success.

While the worst case scenario may be losing critical data to a nation-state that could both undermine a company's business and compromise U.S. national security, losing data to a domestic competitor can also result in significant revenue losses and damage to long-term viability. U.S. corporations must be able to protect their trade secrets from all adversaries to remain competitive.[29] Malicious insiders don't only steal proprietary information to share with companies overseas; they often do so as they prepare to leave their jobs to work for competing companies inside the United States. In one of the most infamous recent cases of such IP theft, an engineer in Google's self-driving car division downloaded thousands of project files before quitting. He immediately started his own autonomous vehicle company, which he sold to Uber—one of Google's top competitors in the market—just months later.[30]

Corporations also deliberately hire employees of competing firms to exploit their knowledge of, and access to, the competitor's IP. In one example, Ticketmaster hired a former employee of Crowdsurge, a rival ticket seller, and used this person's credentials to access Crowdsurge's data and analytics relating to concert ticket pre-sales. Prosecutors asserted that Ticketmaster executives began asking the employee for information related to his former firm within weeks, and that "Ticketmaster employees repeatedly—and illegally—accessed a competitor's computers without authorization using stolen passwords to unlawfully collect business intelligence."[31]

Preventing the loss of proprietary data to U.S.-based industrial competitors can be accomplished through similar measures employed to address foreign-based economic espionage.

TYPES OF INSIDER THREATS

In 2015, INSA's Insider Threat Subcommittee worked closely with the Defense Counterintelligence and Security Agency (DCSA) and ODNI's National Counterintelligence and Security Center (NCSC) to refine the definition of insider threat to be relevant to all U.S. government agencies and private companies. The Subcommittee defines an insider threat as, "The threat posed by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly, or unwittingly, commits acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace."[32]

Countless motivations might drive a person to turn against his or her employer. INSA's Insider Threat Subcommittee identifies several categories of insider threats and outlines the motivating factors that could push a person to steal a company's sensitive data. These include sabotage, theft of intellectual property or national defense information, insider fraud, workplace violence, and unintentional insider threats.[33] Emotional factors that drive malicious insiders include an individual's sense of national pride and politics, financial hardships and disgruntlement. Dissatisfaction at work due to real or perceived unfair treatment can also be manipulated by foreign powers well-versed in the art of espionage.[34]

People with access to sensitive information are not only motivated by a desire to harm an employer they resent , but they frequently take advantage of their access for their own personal gain. In December 2019, for example, a Chinese cancer researcher at a Harvard laboratory was arrested while trying to smuggle vials of cancer cells on a flight to Beijing. His goal was to advance his career by conducting research at a facility in China and publishing study results under his own name.[35] In December 2020, motivated by greed, two married Chinese genetic researchers who developed genetic testing kits at an Ohio hospital pled guilty to selling the kits through a company they formed in China.[36]

It is difficult to identify malicious activity by potential or current insider threat actors before damage is discovered. However, it is possible to identify characteristics typical of individuals indicating personal stress, which might render them susceptible to acting rashly and emotionally. While such traits are not definitive evidence of wrong-doing, they can serve as warning signs.

> External actors' exploitation of unintentional mistakes has been at the root of many large-scale data breaches. In many cases, improving employees' awareness of security threats and best practices can prevent lax behavior that increases risk.

In 2012, the FBI produced an article that focused on common motivations for insider threat actors and observable behaviors that are potential indicators of criminal conduct. The piece highlighted such motivations as financial compensation, divided loyalties, blackmail, and substance abuse. Signs of misdeeds might include such things as taking proprietary or other information without authorization, disregarding company information security policies, unexplained affluence, significant stressful life events, and/or unmet professional expectations.[37]

What is crucial to understanding and recognizing malicious insider threat actors is that they often exhibit indicators that, if identified early, can be mitigated before harm to the organization occurs.[38] The challenge is overcoming peoples' reticence to speak up when these signs are recognized. Additionally, "our natural human tendency is to trust one another, especially our coworkers."[39]

Carnegie Mellon points out that some insiders *unintentionally* open up their employers to risk due to negligence rather than malicious objectives.[40] Employees create risk without an intent to harm through bad business practices, ignorance of policy, lax policy enforcement, a willingness to by-pass security measures to work more efficiently, and just plain human error.[41] Researchers affiliated with Carnegie Mellon University identified four additional categories of unintentional insider threat incidents: accidental disclosure, malicious code introduced through social engineering, theft or improper disposal of records, and loss of portable electronic data storage devices.[42]

Statistically, unintentional insiders (and their unintentional actions) far outnumber the malicious insiders. However, external actors' exploitation of unintentional mistakes has been at the root of many large-scale data breaches. In many cases, improving employees' awareness of security threats and best practices can prevent lax behavior that increases risk.

- In 2011, unintentional employee negligence at RSA Security led to an advanced persistent attack that compromised an estimated 40 million employee records. Two hacker groups working with a foreign government launched phishing attacks targeting RSA employees, pretending to be trusted coworkers and contacts. When employees fell for the attack, the hackers gained access to RSA's networks and were able to compromise SecureID authentication tokens.[43]

- In 2016, the payroll information of roughly 700 current and former Snapchat employees was compromised after a phishing attack tricked a human resources employee into handing over this sensitive information by pretending to be the company's CEO.[44]

- In 2017, Wells Fargo intended to provide a lawyer with a selection of emails and documents related to a case involving a Wells Fargo employee. Instead, the bank accidentally turned over an unencrypted CD with confidential personal and financial information regarding 50,000 of the bank's wealthiest clients.[45]

PROPOSED SOLUTIONS

Despite the prevalent nature of economic espionage throughout U.S. history, the estimated loss of billions of dollars to the American economy each year, and the threat to U.S. national security,[46] a hard push to develop and implement *preemptive*—as opposed to reactive—measures is still lacking. There is no walking back the harm that is done once intellectual property has been compromised. While holding perpetrators, beneficiaries of purloined information, and nation-states accountable is necessary, its effectiveness is weakened by the fact that it does not undo damage already done to American national and economic security.

Proactive steps to protect valuable information can, however, mitigate threats from foreign adversaries and malicious insiders and minimize the damage that they can do.

- The first and most crucial step is to educate corporate and academic leaders about the information and technologies that foreign adversaries want to steal and the steps they may take to do so. The goal is not to discourage or hinder scientifically and commercially valuable collaboration, but rather learn to balance cooperation with security. The FBI, the Intelligence Community, and other government entities routinely brief corporate and academic leaders on these threats, but many of the participants in such briefings are large institutions that have the resources to engage. FBI and others must extend their outreach to more small organizations and labs where a great deal of innovative work is undertaken.
- Companies and universities must also work to instill a culture of security and security *awareness* within their own organizations. Because indicators of potential insider threats often go unrecognized or are ignored by people who are hesitant to report their concerns, corporate and academic leaders must encourage and empower their workforce to come forward when a colleague demonstrates concerning behavior. Organizations should develop and disseminate clear security policies and build awareness of both policies and best practices through steps like posters, periodic training classes, and email campaigns. Employees must know that they can share their concerns with human resources, security staff, and any key stakeholder in the company's insider threat program, including the insider threat hotline if one exists.[47]
- Government agencies should take a more active role in helping companies and institutions of higher education—particularly ones that partner with them on research and development—re-evaluate their security postures and establish comprehensive insider threat programs that are responsive and crafted uniquely to meet industry needs. Agencies can do so by assisting with:
  - > Undertaking capability assessments
  - > Developing security policies and governance structures
  - > Designing and delivering security training
  - > Establishing insider threat awareness programs
- FBI and other agencies do provide this assistance to some companies, but many of them are larger organizations with the capacity to engage the government on such issues on an ongoing basis. Small innovative companies with fewer resources to devote to security policies and programs are in particular need of government advice and assistance.
- Companies and research institutions should also draw on the wide range of insider threat expertise that exists outside of government. Carnegie Mellon's SEI vulnerability assessment processes and methodologies, for example, are valuable tools to strengthen insider threat programs.

CONCLUSION

The economic lifeblood of any society is innovation—the creation of new techniques, tools, or processes that are relied on for the betterment of its citizens. Foreign adversaries will always seek information regarding commercially valuable innovations, and they will target and recruit knowledgeable insiders who understand the significance of sensitive data and have unimpeded access to it. Thefts of such data harm American economic competitiveness and national security.

The fundamental defenses against insider threats are employee education and continuous encouragement of the workforce to raise concerns when circumstances appear to be unusual, out of place, or troubling. If people do not understand the significance of the threat posed by those with nefarious intentions, they cannot help protect their organizations' intellectual property.

A better understanding of malicious insiders' motivations, more robust public-private collaboration, and effective employee training and awareness strategies can hinder foreign attempts to steal commercially valuable intellectual property and protect U.S. national and economic security.

REFERENCES

[1]*The Federal Bureau of Investigation (FBI) defines economic espionage as, "foreign power-sponsored or coordinated intelligence activity directed at the U.S. Government (USG) or U.S. corporations, establishments, or persons, designed to unlawfully or clandestinely influence sensitive economic policy decisions or to unlawfully obtain sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies."*

[2]*National Bureau of Asian Research, "Update to the IP Commission Report," February 2017. At https://www.documentcloud.org/documents/5737506-IP-Commission-Report-Update-2017.html.*

[3]*Federal Reserve Bank of St. Louis, Gross Domestic Product. At https://fred.stlouisfed.org/series/GDP.*

[4]*18 USC 1831. At https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter90&edition=prelim.*

[5]*US Department of Justice, "Introduction to the Economic Espionage Act," Criminal Resource Manual (CRM), Sec. 1122. June 2015. At https://www.justice.gov/jm/criminal-resource-manual-1122-introduction-economic-espionage-act. See also 18 USC 1832.*

[6]*National Counterintelligence and Security Center (NCSC), "NCSC Unveils the National Counterintelligence Strategy of the US 2020-2022", press release, February 10, 2020. At Https://dni.gov/index.php/newsroom/press-releases/item/2098-ncsc-unveils-the-national-counterintelligence-strategy-of-the-u-s-2020-2022*

[7]*Office of the National Counterintelligence Executive, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011," October 2011. At https://www.odni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf.*

[8]*"Foreign Economic Espionage in Cyberspace," National Counterintelligence and Security Center, 2018. At https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.*

[9]*Carnegie-Mellon University Software Engineering Institute, "Our Research: Insider Threat," no date. At https://www.sei.cmu.edu/our-work/insider-threat/.*

[10]*Carnegie-Mellon University Software Engineering Institute, CERT Insider Threat Center, "Common Sense Guide to Mitigating Insider Threats, Fifth Edition," December 2016. At https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf.*

[11]*Congressional Research Service, U.S. Research and Development Funding and Performance: Fact Sheet, Report R44307, January 24, 2020. At https://fas.org/sgp/crs/misc/R44307.pdf.*

[12]*Erik Sherman, "One in Five U.S. Companies Say China Has Stolen Their Intellectual Property," Fortune, March 1, 2019. At https://fortune.com/2019/03/01/china-ip-theft.*

[13]*Gina Heeb, "FBI Says It Opens New Espionage Investigation Into China 'Every 10 Hours'," Forbes, April 14, 2021. At https://www.forbes.com/sites/ginaheeb/2021/04/14/fbi-says-it-opens-new-espionage-investigation-into-china-every-10-hours/?sh=772b1c707a5d.*

[14]*Congressional Research Service, "Made in China 2025" Industrial Policies: Issues for Congress, August 11, 2020. At https://fas.org/sgp/crs/row/IF10964.pdf.*

[15]*U.S. Attorney's Office for the Eastern District of Texas, U.S. Department of Justice, "China Initiative," website, September 1, 2020. At https://www.justice.gov/usao-edtx/china-initiative.*

[16]*For a list of 68 indictments related to the China Initiative, see Department of Justice, "Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018," website, November 12, 2020. At https://www.justice.gov/opa/information-about-department-justice-s-china-initiative-and-compilation-china-related.*

[17]*Steve Patterson," Jacksonville-Based Navy officer, Wife Indicted in Chinese Smuggling Scheme," Florida Times-Union, November 1, 2019. At https://www.jacksonville.com/news/20191101/jacksonville-based-navy-officer-wife-indicted-in-chinese-smuggling-scheme. See also U.S. Department of Justice, "Jacksonville Woman Pleads Guilty to Attempting to Illegally Exporting Maritime Raiding Craft and Engines to China," press release, September 16, 2020. At https://www.justice.gov/opa/pr/jacksonville-woman-pleads-guilty-attempting-illegally-exporting-maritime-raiding-craft-and.*

[18]*U.S. Department of Justice, "Chinese Energy Company, U.S. Oil & Gas Affiliate and Chinese National Indicted for Theft of Trade Secrets," press release, October 29, 2020. At https://www.justice.gov/opa/pr/chinese-energy-company-us-oil-gas-affiliate-and-chinese-national-indicted-theft-trade-secrets.*

[19]*U.S. Department of Justice, " Researcher Charged with Illegally Using U.S. Grant Funds to Develop Scientific Expertise for China," press release, July 9, 2020. At https://www.justice.gov/opa/pr/researcher-charged-illegally-using-us-grant-funds-develop-scientific-expertise-china.*

[20]*Ellen Barry and Gina Kolata, "China's Lavish Funds Lured U.S. Scientists. What Did It Get in Return?" New York Times, February 6, 2020. At https://www.nytimes.com/2020/02/06/us/chinas-lavish-funds-lured-us-scientists-what-did-it-get-in-return.html.*

[21]*Permanent Subcommittee on Investigations, Committee on Homeland Security and Government Affairs, U.S. Senate, Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans," November 18, 2019, p. 6. At https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans.pdf. James Jin Kang, "The Thousand Talents Plan Is Part of China's Long Quest to Become the Global Scientific Leader," The Conversation, August 31, 2020. At https://theconversation.com/the-thousand-talents-plan-is-part-of-chinas-long-quest-to-become-the-global-scientific-leader-145100.*

[22]*U.S. Department of Justice, "Senior NASA scientist pleads guilty to making false statements related to Chinese Thousand Talents Program participation and professorship," press release, January 13, 2021. At https://www.justice.gov/usao-sdny/pr/senior-nasa-scientist-pleads-guilty-making-false-statements-related-chinese-thousand.*

[23]*U.S. Department of Justice, "Harvard University Professor Indicted on False Statement Charges," press release, June 9, 2020. At https://www.justice.gov/opa/pr/harvard-university-professor-indicted-false-statement-charges. See also Aruna Viswanatha and Kate O'Keeffe, "Harvard chemistry chairman charged on alleged undisclosed ties to China," The Wall Street Journal, January 28, 2020. At https://www.wsj.com/articles/harvards-chemistry-chair-charged-on-alleged-undisclosed-ties-to-china-11580228768.*

[24]*Gina Kolata, "Vast Dragnet Targets Theft of Biomedical Secrets for China," New York Times, November 4, 2019. At https://www.nytimes.com/2019/11/04/health/china-nih-scientists.html. See also Brad Racino and Jill Castellano, "UCSD doctor resigns amid questions about undisclosed Chinese businesses," inewsource, June 6, 2019. At https://inewsource.org/2019/07/06/thousand-talents-program-china-fbi-kang-zhang-ucsd/.*

[25]*Michelle van Cleave, Statement before the House Committee on Science, Space, and Technology Subcommittee on Oversight, Subcommittee on Research and Technology, "Scholars or Spies: Foreign Plots Targeting America's Research and Development," hearing, April 11, 2018. At https://www.govinfo.gov/content/pkg/CHRG-115hhrg29781/pdf/CHRG-115hhrg29781.pdf.*

[26]*Elizabeth Redden, Elizabeth, "Science vs. Security," Inside Higher Ed, April 16, 2019. At https://www.insidehighered.com/news/2019/04/16/federal-granting-agencies-and-lawmakers-step-scrutiny-foreign-research.*

[27]*Gina Kolata, "Vast Dragnet Targets Theft of Biomedical Secrets for China," New York Times, November 4, 2019. At https://www.nytimes.com/2019/11/04/health/china-nih-scientists.html.*

[28]*Redden (2019).*

[29]*Statements on Introduced Bills and Joint Resolutions, S. Doc. (Mar. 30, 2011). https://fas.org/irp/congress/2011_cr/s678.html*

[30]*U.S. Department of Justice, "Former Uber Executive Sentenced to 18 Months in Jail for Trade Secret Theft from Google," press release, August 4, 2020. At https://www.justice.gov/usao-ndca/pr/former-uber-executive-sentenced-18-months-jail-trade-secret-theft-google. See also Nick Statt, "Former Google exec Anthony Levandowski Sentenced to 18 Months for Stealing Self-Driving Car Secrets," The Verge, August 4, 2020. At https://www.theverge.com/2020/8/4/21354906/anthony-levandowski-waymo-uber-lawsuit-sentence-18-months-prison-lawsuit.*

[31]*Bruce Sussman, "Ticketmaster hacked competitor to steal data and analytics, fined millions," Secureworld, January 4, 2021. At https://www.secureworldexpo.com/industry-news/ticketmaster-hacked-competitor-to-steal-data-analytics.*

[32]*Intelligence and National Security Alliance, "Explanation of INSA-Developed Insider Threat Definition," December 3, 2018 (2018). At https://www.insaonline.org/wp-content/uploads/2018/10/INSA_InsiderThreat_definition-Flyer.pdf.*

[33]*Intelligence and National Security Alliance, "Categories of Insider Threats," October 10, 2019. At https://www.insaonline.org/wp-content/uploads/2019/10/INSA_WP_Categories_of_Insider_Threats-1.pdf.*

[34]*ObserveIT, "The Primary Factors Motivating Insider Threats," September 17, 2019. At https://www.observeit.com/blog/primary-factors-motivating-insider-threats/.*

[35]*Ellen Barry, "Stolen Research: Chinese Scientist Is Accused of Smuggling Lab Samples," New York Times, December 31, 2019. At https://www.nytimes.com/2019/12/31/us/chinese-scientist-cancer-research-investigation.html.*

[36]*Department of Justice, "Man Who Worked at Local Research Institute for 10 Years Pleads Guilty to Conspiring to Steal Trade Secrets, Sell Them in China," press release, December 11, 2020. At https://www.justice.gov/opa/pr/man-who-worked-local-research-institute-10-years-pleads-guilty-conspiring-steal-trade-secrets/.*

[37]*Federal Bureau of Investigation, "Economic Espionage: How to Spot a Possible Insider Threat," May 11, 2012. At https://www.fbi.gov/news/stories/how-to-spot-a-possible-insider-threat.*

[38]*Defense Security Service Counterintelligence Directorate, "Insider Threat: Combating the Enemy within Your Organization," no date. At https://home.army.mil/bragg/application/files/3215/0515/6485/InsiderThreat.pdf.*

[39]*Rick Ensenbach, "Insider Threats: Are You Ignoring the Human Risk in Your Information Security Program?" January 21, 2016. At https://www.wipfli.com/insights/articles/cons-hc-insider-threats-are-you-ignoring-the-human-risk-in-your-information-security-program.*

[40]*CERT defines unintentional insider threats as, "current or former employees, contractors, or other business partners who…[have] or had authorized access to an organization's network, system, or data" yet "had no malicious intent associated with his or her action (or inaction) that caused harm or substantially increased the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems." See Cappelli, Moore, and Trzeciak (2012). See also Carnegie Mellon University Software Engineering Institute, CERT Insider Threat Team, "Unintentional Insider Threats: A Foundational Study," August 2013. At https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf.*

[41]*"Human error" is itself a broad category that includes deficiencies in work setting (such as insufficient resources, poor management systems, and inadequate security practices), work planning and controls (such as job pressure, time factors, task difficulty, change in routine, and poor task planning and management), and employee readiness (such as inattention, stress, fatigue, boredom, illness, and injury).*

[42]*Frank L. Greitzer, Jeremy Strozer, Sholom Cohen, John Bergey, Jennifer Cowley, Andrew Moore, and David Mundie, "Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies," 2014 47th Hawaii International Conference on System Sciences, Waikoloa, Hawaii, 2014, pp. 2025-2034. At https://ieeexplore.ieee.org/document/6758854.*

[43]*ObserveIT, "5 examples of insider-threat caused breaches that illustrate the scope of the problem," March 22, 2018. At https://www.observeit.com/blog/5-examples-of-insider-threat-caused-breaches/.*

[44]*A. Hern, "Snapchat leaks employee pay data after CEO email scam," The Guardian, February 29, 2016. https://www.theguardian.com/technology/2016/feb/29/snapchat-leaks-employee-data-ceo-scam-email.*

[45]*Serge F. Kovaleski and Stacy Cowley, "Wells Fargo Accidentally Releases Trove of Data on Wealthy Clients," New York Times, July 21, 2017. At https://www.nytimes.com/2017/07/21/business/dealbook/wells-fargo-confidential-data-release.html.*

[46]*Federal Bureau of Investigation, "Economic Espionage: FBI Launches Nationwide Awareness Campaign," July 23, 2015. At https://www.fbi.gov/news/stories/economic-espionage.*

[47]*For more insights on the importance of human resources staffs as a "first line of defense" in identifying and mitigating insider threats, see Intelligence and National Security Alliance, Human Resources and Insider Threat Mitigation: A Powerful Pairing, September 2020. At https://www.insaonline.org/just-released-new-insider-threat-intelligence-insights/.*

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Vinny Corsi, *IBM; Insider Threat Subcommittee Chair*

Sue Steinke, *Peraton;*
Insider Threat Subcommittee Vice Chair

Cathy Albright, *Thomson Reuters Special Services, LLC*

Scott Alston

Joe Hoofnagle, *Social Security Administration*

Josh Massey, *MITRE Corporation*

Eric Schuck, *Thomson Reuters Special Services, LLC*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor,
Director of Communications and Policy

Caroline Henry,
Marketing and Communications Assistant

Rachel Greenspan, *Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. Our 160+ member organizations and its 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S INSIDER THREAT SUBCOMMITTEE

INSA's Insider Threat Subcommittee researches, discusses, analyzes, and assesses counterintelligence and insider threat issues that affect government agencies, cleared contractors, and other public and private sector organizations. The Subcommittee works to enhance the effectiveness, efficiency, and security of government agencies and their industry partners, as well as to foster more effective and secure partnerships between the public, private and academic sectors.