Policy Analysis

CATO INSTITUTE

February 9, 2021 | Number 909

Espionage, Espionage-Related Crimes, and Immigration

A Risk Analysis, 1990–2019

By Alex Nowrasteh

EXECUTIVE SUMMARY

Espionage poses a threat to national security and the private property rights of Americans. The government should address the threat of espionage in a manner whereby the benefits of government actions taken to reduce it outweigh the costs of those actions. To aid in that goal, this policy analysis presents the first combined database of all identified spies who targeted both the U.S. government and private organizations on U.S. soil. This analysis identifies 1,485 spies on American soil who, from 1990 through the end of 2019, conducted state or commercial espionage. Of those, 890 were foreign-born, 583 were native-born Americans, and 12 had unknown origins.

The scale and scope of espionage have major implications for immigration policy, as a disproportionate number of the identified spies were foreign-born. Native-born Americans accounted for 39.3 percent of all spies, foreign-born spies accounted for 59.9 percent, and spies of unknown origins accounted for 0.8 percent. Spies who were born in China, Mexico, Iran, Taiwan, and Russia account for 34.7 percent of all spies. The chance that a native-born American committed espionage or an espionage-related crime and was identified was about 1 in 13.1 million per year from 1990 to 2019. The annual chance that a foreign-born person in the United States committed an espionage-related crime and was discovered doing so was about 1 in 2.2 million during that time. The government was the victim in 83.3 percent of espionage cases, firms were the victims of commercial espionage in 16.3 percent of the cases, and hospitals and universities were the victims of espionage in 0.1 percent and 0.3 percent of the cases, respectively.

The federal government should continue to exclude foreign-born individuals from entering the United States if they pose a threat to the national security and private property rights of Americans through espionage. A cost-benefit analysis finds that the hazards posed by foreign-born spies are not large enough to warrant broad and costly actions such as a ban on travel and immigration from China, but they do warrant the continued exclusion of potential spies under current laws.

Alex Nowrasteh is the director of immigration studies at the Cato Institute's Center for Global Liberty and Prosperity. He is the coauthor (with Benjamin Powell) of the book *Wretched Refuse? The Political Economy of Immigration and Institutions* (Cambridge University Press, 2020). The author thanks Maxwell Tabarrok for research assistance.

"The scale and scope of espionage have major implications for immigration policy because a disproportionate number of the identified spies were foreign-born."

INTRODUCTION

Espionage and espionage-related crimes pose a threat to national security and the private property rights of Americans. There were 1,485 identified spies on American soil from 1990 through the end of 2019 who conducted state and commercial espionage. Of those, 890 were foreign-born, 583 were native-born Americans, and 12 had unknown origins. This policy analysis presents the first combined database of all identified spies who targeted the U.S. government (henceforth "state espionage") and private organizations (henceforth "commercial espionage") on U.S. soil (see Annex at https://infogram.com/annex-identified-spies-on-us-soil-1990-2019-1hd12y8p0rem4km?live).

The scale and scope of espionage have major implications for immigration policy because a disproportionate number of the identified spies were foreign-born. Native-born Americans accounted for 39.3 percent of all spies, foreign-born spies accounted for 59.9 percent, and spies of unknown origins accounted for 0.8 percent. Spies who were born in China, Mexico, Iran, Taiwan, and Russia accounted for 34.7 percent of all spies. There were 184 spies born in China, who accounted for 12.4 percent of all spies. Mexicans accounted for 172 spies, or 11.6 percent, and many violated the Arms Export Control Act (AECA) by primarily selling weapons to drug cartels and other criminal organizations. The 84 Iranians in the database comprised 5.7 percent of all spies; many of them were guilty of violating the U.S. economic embargo on Iran. The next two largest groups of spies were 41 Taiwanese and 35 Russians, comprising 2.8 percent and 2.4 percent, respectively.

The chance that a native-born American committed espionage or an espionage-related crime and was identified was about 1 in 13.1 million per year from 1990 to 2019. The annual chance that a foreign-born person in the United States committed an espionage-related crime and was discovered doing so was about 1 in 2.2 million during that time. The government was the victim in 83.3 percent of instances of espionage, with violators of the AECA accounting for more than 65.7 percent of espionage or espionage-related offenses against the government. American firms were the victims of commercial espionage 16.3 percent of the time, while hospitals and universities were the victims of espionage 0.1 percent and 0.3 percent of the time, respectively.

The federal government has an important role in limiting espionage and in excluding foreign-born individuals from entering the United States if they pose a threat to the national security and private property rights of Americans through espionage. This analysis of government and commercial spies can aid in the efficient allocation of scarce government anti-espionage resources to their most highly valued uses. A cost-benefit analysis finds that the hazards posed by foreign-born spies are not large enough to warrant broad and costly actions such as a ban on travel and immigration from China, but they do warrant the continued exclusion of potential spies under current laws.

BACKGROUND

State espionage is broadly the act of obtaining information or items that are not publicly available from the U.S. government in the interests of a foreign government or in service of a broader ideological goal.[1] Broadly, commercial espionage is the act of unlawfully and clandestinely obtaining valuable proprietary information; intellectual or other property; or financial, trade, or economic information from American firms, establishments, or persons for one's personal benefit or the benefit of another domestic firm, foreign firm, foreign government, or other entity, foreign or domestic.[2] When the U.S. government is the direct victim, it is state espionage. Commercial espionage is when nonstate entities are the direct victims. Espionage can be conducted electronically or from a distance, such as through computer hacking or via spy satellites and the interception of signals, or via human spies. This report focuses entirely on human espionage carried out by spies on American soil, as that is the type of espionage affected by immigration policy.

Effectiveness of State and Commercial Espionage

State espionage is a well-known threat to national security. The theft of government secrets can harm America's military and reduce the effectiveness of its defense against a foreign adversary. The Chinese military strategist Sun Tzu wrote that "what enables intelligent government and a wise military leadership to overcome others and achieve extraordinary accomplishments is foreknowledge."[3] History provides many instances of foreknowledge gathered by human espionage that gave a decisive advantage to the United States. During the Cold War, Col. Oleg Penkovsky in Soviet military intelligence provided important information to the Central Intelligence Agency (CIA) on Soviet operational plans and missile technology that was crucial to understanding that the Soviet arms buildup on Cuba in 1962 included medium-range and intermediate-range ballistic missile facilities.[4] The intelligence from Penkovsky was essential to helping the United States peacefully prevail in the Cuban Missile Crisis because it alerted the U.S. government to the Soviet intentions prior to the installation of the nuclear ballistic missiles.[5] American national security information related to the quality, quantity, and vulnerabilities of the U.S. military would be very valuable to a potential foreign adversary and weaken American national defense.

Commercial espionage presents a different type of threat because it could potentially reduce the quality of America's national security in the long run by diminishing its technological superiority on the battlefield and its economic advantages elsewhere. Consequently, commercial espionage is emerging as a relatively larger concern in the 21st century than it was in the 20th century. Commercial espionage is a more important national security concern than it was during the Cold War, when the Soviet Union's commercial espionage efforts weren't well known until about a decade before it collapsed.[6] Although commercial espionage can be a threat, state-supported commercial espionage is a sign of weakness and a lack of dynamism. In 2020, Chinese Premier Li Keqiang admitted as much when he said, "Our capacity for innovation is not strong, and our weakness in terms of core technologies for key fields remains a salient problem."[7] Doctor and writer Steven Novella echoed Premier Li's point when he wrote:

> There is also legitimate concern that totalitarian governments do not create an environment in which science can flourish. Science requires transparency, it requires valuing method over results, and it should be ideologically neutral. These are not concepts that flourish under a totalitarian regime. Also, the scientists who get promoted to positions of respect and power are likely to be those who please the regime, by proving, for example, that their cultural propaganda is real. So the selective pressures for advancement do not prioritize research integrity.[8]

The result is rampant fraud in Chinese scientific institutions that undermines scientific and technological progress. Academic psychologist Stuart Ritchie documents the situation well when he lists numerous surveys of Chinese scientists who allege that a large percentage of research by their colleagues is a result of scientific misconduct and that scientific authorities do almost nothing about these cases.[9] In another instance identified by Ritchie, a 2009 review of studies that claimed to use randomized controlled trials found that only 7 percent of the trials actually were.[10]

The Chinese government isn't the only government with serious institutional weaknesses that has sought to ameliorate its problem through espionage. During the Cold War, the Soviet Union and Soviet satellite states engaged in commercial espionage to narrow the technological and economic gap.[11] While it was by no means their focus of espionage, commercial espionage did achieve some notable successes for communist governments prior to their collapse. The most striking success was East Germany's

"During the Cold War, the Soviet Union and Soviet satellite states engaged in commercial espionage to narrow the technological and economic gap."

> "Allegations of espionage against the United States conducted by agents of China prompted the U.S. Department of Justice to create the China Initiative in 2018."

commercial espionage program targeting West Germany. Economists Albrecht Glitz and Erik Meyersson investigated the East Germany economic returns to commercial espionage over the 1970–1989 period by linking information from East Germany's foreign intelligence service to the sectors of the West Germany economy that were spied on. Using that information, they then estimated how the intelligence that was gathered affected the sector-specific gaps in total factor productivity (TFP) between the countries. They found big effects, such that the East German/West German TFP ratio would have been 13.3 percent lower at the end of the Cold War had East Germany not engaged in industrial espionage in the West.[12] Those gains are substantial but were "driven by relatively few high-quality pieces of information and particularly large in sectors closer to the West German technological frontier."[13] The return on investment to East Germany for commercial espionage was very high, at around €4.6 billion in 1988, compared with annual spying expenditures of about €6.4 million.[14]

Although the return for commercial espionage appears impressive at first sight, it had an enormous and hidden long-run cost because it reduced investment in technological and scientific development in East Germany. Meyersson said that commercial espionage is "R&D on cocaine. . . . Maybe you can have a little bit of fun with it, but it's not good for you in the long run." Commercial espionage is "a way to keep up. . . . It's not a strategy to become a world leader," said Meyersson. Eventually, the productivity returns of commercial and technological secrets stolen by East Germany fell to near zero because the secrets were too advanced to improve the country's more primitive industry. One of the more successful East German spies made a comment to his case officer that summarizes the problem: "I'm giving you the best technology available, why can't you use it?"[15]

The U.S. Response to Chinese Espionage

Allegations of espionage against the United States conducted by agents of the People's Republic of China prompted the U.S. Department of Justice (DOJ) to create the China Initiative in 2018 to focus on detecting, prosecuting, and stopping Chinese espionage.[16] The DOJ is leading the initiative, but it is a government effort that includes multiple agencies using the vast powers of the federal government to achieve the following stated goals:

- Identify priority trade secret theft cases, ensure that investigations are adequately resourced, and work to bring them to fruition in a timely manner and according to the facts and applicable law;
- Develop an enforcement strategy concerning non-traditional collectors (e.g., researchers in labs, universities and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests;
- Educate colleges and universities about potential threats to academic freedom and open discourse from influencing efforts on campus;
- Apply the Foreign Agents Registration Act to unregistered agents seeking to advance China's political agenda, bringing enforcement actions when appropriate;
- Equip the nation's U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their Districts and support their outreach efforts;
- Implement the Foreign Investment Risk Review Modernization Act (FIRRMA) for the DOJ (including by working with Treasury to develop regulations under the statute and prepare for increased workflow);
- Identify opportunities to better address supply chain threats, especially those impacting the telecommunications sector, prior to the transition to 5G networks;
- Identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses;

- Increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States; and
- Evaluate whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.[17]

In 2020, Attorney General William Barr said, "The People's Republic of China is now engaged in an economic blitzkrieg—an aggressive, orchestrated, whole-of-government (indeed, whole-of-society) campaign to seize the commanding heights of the global economy and to surpass the United States as the world's preeminent technological superpower."[18] The DOJ's China Initiative covers hacking from abroad, importation of counterfeit goods, illegal export by people abroad, foreign firms charged with crimes, and other espionage activities not covered in this analysis because the spies are not physically present on American soil and therefore have no nexus to immigration policy.[19] To date, DOJ attorneys and nongovernmental research have presented numerous anecdotes about Chinese espionage but little to no verifiable data on the number of cases against Chinese spies or spies from other countries as a point of comparison.[20]

In response to the threat of Chinese espionage, the government has also put additional restrictions on the issuance of student visas to Chinese nationals. They must reapply annually if they are graduate students in sensitive research fields. Visas are prohibited for Chinese students from universities affiliated with the People's Liberation Army (PLA).[21] The government has also revoked the visas of more than 1,000 Chinese students who may have ties to the PLA or PLA-affiliated universities.[22] The National Institutes of Health has launched an investigation into scientists with foreign ties to discover violations of the terms of their government grants, particularly among Chinese-born researchers.[23] In July 2020, the Trump administration closed the Chinese consulate in Houston, claiming that it was aiding Chinese-born scientists in committing commercial espionage.[24] The government has also designated the roughly 75 Chinese-government funded Confucius Institutes in the United States as part of its "propaganda apparatus."[25]

The government's fear of Chinese espionage has even extended to potentially banning the popular Chinese-owned web application TikTok and the messaging app WeChat because the government claims they could be used to conduct espionage.[26] There is currently no evidence that TikTok and WeChat facilitate espionage, that they increase the chance of espionage, or that they have ever been used by Chinese intelligence services.[27] These allegations may prove to be true, but it's important that policymakers and the public have evidence of that before the government imposes such a high cost on a foreign firm and its American consumers.[28] After initially announcing the impending ban of TikTok and WeChat, the Trump administration said that it would allow TikTok to remain operational in the United States if it was at least partly sold to a U.S. firm and if the U.S. government got a share of the money.[29] The government dropped the demand for a cut of the deal, TikTok hasn't been sold to an American firm, and it was still available in the United States at the end of the Trump administration.[30]

The ombudsman of U.S. Citizen and Immigration Services (USCIS) warned that the Optional Practical Training (OPT) program, which allows some foreign-born students in the science, technology, engineering, and mathematics (STEM) fields to train and work lawfully for up to three years after their graduation, could be "leveraged by foreign governments as a means of conducting espionage or illicit technology transfer in the STEM areas."[31] The USCIS report is long on potential problems and short on evidence, but it is nonetheless a remarkable warning by a non-intelligence agency.

Many commentators and policymakers think U.S. policies should go further in

"In response to the threat of Chinese espionage, the government has also put additional restrictions on the issuance of student visas to Chinese nationals."

"The Chinese government clearly has the intention to engage in espionage but not necessarily the capability to do so effectively."

restricting Chinese immigration in response to the threat of espionage. Oren Cass, executive director of the think tank American Compass, has called for reducing the number of Chinese students admitted until China changes policies that harm American companies, including its support of commercial espionage.[32] Sen. Ted Cruz (R-TX) introduced the Protecting America from Spies Act to redundantly exclude foreign-born spies from the United States.[33] Sens. Tom Cotton (R-AR) and Marsha Blackburn (R-TN) introduced the Secure Campus Act to prohibit Chinese nationals from receiving visas to the United States for graduate or post-graduate studies in STEM fields to stop commercial espionage from China.[34]

The Trump administration embraced economic protectionism, and the above policies are perfectly consistent with that agenda.[35] If one were to hear about the above policies in a vacuum without the espionage-related justifications, one could be forgiven for thinking that economic protectionism was the real reason behind them. The government claims that its actions are in response to the threat of Chinese espionage even when they are indistinguishable from normal economic protectionism, but there is evidence that the Chinese government is supporting a significant amount of state and commercial espionage in the United States.

Chinese Espionage

The Chinese government has a large, well-developed, and aggressive state intelligence system. The main Chinese government agencies devoted to state espionage are the Chinese Ministry of State Security (MSS) and the PLA.[36] In addition, they have a large variety of programs that likely incentivize commercial espionage. Thus, the scale of Chinese intelligence operations is potentially much larger than the size or effectiveness of its government intelligence agencies would suggest.[37]

Many intelligence analysts use a metaphor to compare Chinese intelligence to other countries:

> If a beach was an espionage target, the Russians would send in a sub, frogmen would steal ashore in the dark of night and with great secrecy collect several buckets of sand and take them back to Moscow. The Americans would target the beach with satellites and produce reams of data. The Chinese would send in a thousand tourists, each assigned to collect a single grain of sand. When they returned, they would be asked to shake out their towels. And they would end up knowing more about the sand than anyone else.[38]

Despite numerous problems with the beach metaphor, there are probably a lot of Chinese spies who are mostly amateurs and not well skilled at espionage but who have subject-matter expertise in their individual professions.[39] Thus, highly trained and technical workers in U.S. firms, universities, research institutes, and hospitals can identify valuable intelligence but are not well trained in collecting it, which likely leads to a large number of them being caught because they are making amateurish mistakes. The Chinese government clearly has the intention to engage in espionage but not necessarily the capability to do so effectively, which is potentially why it's playing a numbers game by trying to recruit and incentivize many commercial spies, who will mostly fail but who will achieve enough success so that the benefits of the effort exceed the costs—at least in the short run.[40]

The Chinese government has many ambitious economic plans to modernize and develop science and technology production domestically in collaboration with foreign researchers, sometimes at the expense of the Chinese government, and often by recruiting talent and paying for scientific publications. The Chinese government's Made in China 2025 initiative aims for government-selected sectors of the economy to be less reliant on imports. Its long-run goal is for China to be the world leader in science and technology development by 2050. To support this,

the Chinese government has more than 200 talent-recruitment plans to increase the quality of human capital in China. They include, potentially, the Chinese-government funded Confucius Institutes that mainly try to propagandize for China at foreign universities where hundreds of thousands of Chinese students are studying, as well as the Thousand Talents Program.[41] According to one report:

> China designed the Thousand Talents Plan to recruit 2,000 high-quality overseas talents, including scientists, engineers, entrepreneurs, and finance experts. The plan provides salaries, research funding, lab space, and other incentives to lure experts into researching for China. According to one report, by 2017, China dramatically exceeded its recruitment goal, having recruited more than 7,000 "high-end professionals," including several Nobel laureates.[42]

China-born researchers who return to China with technical know-how and information from abroad have an advantage in getting jobs and funding for their research. That could incentivize commercial espionage for scientists who are abroad, even though they do not have an explicit espionage mandate and there is only fragmentary evidence that government benefits for returning are used to further commercial espionage.[43]

These incentives also have perverse effects on the quality of Chinese scientific and technological research. Until recently, Chinese universities paid researchers for each publication in academic journals, which encouraged more publications but not necessarily better research. The Chinese government recently banned cash payments for publications because it produced the perverse incentive to engage in questionable research practices that contributed to systemic fraud problems in Chinese research and the production of many low-quality publications.[44]

A prime example of the latter is the publication record of a Professor Gao from Heilongjiang University who published 279 articles in a single journal and received half of all the cash rewards for publication from his university between 2004 and 2009. His papers were about new crystal structures that he developed in the lab. The papers could have all been combined into a single paper, but he separated them into 279 different papers to maximize his cash reward.[45] It's unlikely that state-directed scientific research like this will make China a world leader in science and technology, because even though the cash payments have been canceled, China remains a totalitarian country that quashes the type of open debate necessary to make sustained technological advances.

As one example, it's very unlikely that independent Chinese researchers would examine whether Chinese government efforts to direct scientific research are successful because a negative finding would expose a government program as ineffective and embarrass the government of a totalitarian state—with negative personal ramifications for the researchers. The incentives of researchers in China are to support the government's policies and research agenda with their work, even if they are ineffective or inefficient. However, stolen defense technology could narrow the technological gap between the United States and China enough to make a major difference on a potential future battlefield.

The Scale of Foreign Espionage

Despite the stated worries of U.S. government officials and their numerous efforts to reduce espionage, especially from China, they have not released a comprehensive list of spies or espionage to show how pervasive the problem is. Government agencies that counter espionage have many anecdotes, many of them very scary, but efficient public policy cannot be anecdote-driven if it is to be successful.[46] Anecdotes cannot even tell us if there is a problem to solve. It is in the best interests of national security for the government to release more data on espionage in order to convince the American public and the world that

"It is in the best interests of national security for the government to release more data on espionage."

"This analysis focuses on espionage and espionage-related crimes during the 30-year period from January 1, 1990, to December 31, 2019."

espionage poses a risk as serious as the government claims. Without such information, public support for anti-espionage activities could diminish.[47] Additionally, if the release of such information shows that the government has inflated the risk from espionage, then it is in the national security interest of the United States to reallocate scarce anti-espionage resources away from smaller threats toward more serious ones. Either way, more publicly available data are essential to identifying actual threats, avoiding threat inflation or deflation, and efficiently allocating resources to maximize national security, given budget constraints.

Thus, this policy analysis presents the first accounting and analysis of state and commercial espionage in the United States in the 1990–2019 period. Hopefully, this analysis will inform the public debate over espionage, identify how serious a problem it is, be a first step toward quantifying the potential scale of the problem, and help the government to efficiently respond to espionage threats.

METHODOLOGY

This analysis focuses on espionage and espionage-related crimes during the 30-year period from January 1, 1990, to December 31, 2019, thus largely excluding espionage from the Cold War and ending with the last full year of available data. It identifies spies who conducted espionage on American soil by their countries of origin (regardless of how long they lived in the United States); their ethnicities; their specific crimes; their victims; the countries that benefited from the espionage; whether the spies worked for the U.S. government; whether the offenses were commercial espionage or state espionage, as defined in this analysis; and the dates of their first known contacts with law enforcement or when indictments were filed against them. Prior to 2020, Hong Kong is counted as a separate country of origin, but Hong Kongers are ethnically Chinese. Taiwan is coded as a separate country and ethnic group. Information on the visa that foreign-born spies used to initially enter the United States is inconsistently reported and omitted from the analysis but is included in the Annex at https://infogram.com/annex-identified-spies-on-us-soil-1990-2019-1hd12y8p0rem4km?live.

This analysis includes spies who were convicted of espionage or espionage-related offenses, who were arrested for those offenses but who have not yet faced trial, who committed suicide after they were identified, or who are currently wanted and at large if they spied while on U.S. soil. It includes spies who were spying on government agencies, those who committed commercial espionage, and whistleblowers. The analysis casts a large net to capture a wide and potentially overinclusive definition of espionage because it is better to overcount spies than to undercount them.

Spies must have been on American soil during some period when they were engaged in espionage or espionage-related activities. Spies who carried out their espionage from abroad, never set foot on U.S. soil, or were arrested by foreign governments and extradited to the United States without previously having been inside the United States are not included. For commercial espionage, this analysis includes individuals charged with those crimes if their trials haven't commenced yet. It does not count individuals sued in civil actions over theft of trade secrets, nor does it count firms convicted of commercial espionage.[48] Where conflicting information exists as to whether individuals were spies or set foot on U.S. soil during the time that they were engaged in espionage, this analysis includes them to err on the side of maximizing the number of spies.

This analysis assumes that foreign-born spies intend to spy for their home countries unless otherwise indicated. If the spy was apprehended in a sting operation where the law enforcement authorities pretended to be from a specific foreign government, then that foreign country is the intended beneficiary.[49] In the cases of commercial espionage, when a foreign-born or native-born spy steals a trade secret to make money by establishing a firm or attempting to otherwise profit inside of the United States,

the beneficiary is coded as "personal gain" or as the United States. If the commercial espionage is used to establish a firm in a foreign country, then that country is coded as the intended beneficiary of the espionage. If the intended beneficiary of the espionage is al Qaeda, then it is coded as al Qaeda because it is a global terrorist network, but other regional terrorist organizations, drug cartels, or insurgents who are the intended beneficiaries are coded as the countries in which they primarily operate. For instance, espionage conducted for the benefit of Hezbollah is coded as benefiting Lebanon, and espionage that benefits Mexican drug cartels is coded as benefiting Mexico.

In this analysis, state espionage includes these specific crimes: conspiracy to defraud the U.S. government;[50] unlawful retention or communication of national defense information;[51] gathering or delivering of defense information to aid a foreign government;[52] photographing or sketching defense installations;[53] being an unregistered agent of a foreign government;[54] having unauthorized access to a computer;[55] producing nuclear materials outside the United States and other violations of the Atomic Energy Act;[56] violations of the Intelligence Identities Protection Act;[57] and theft, bribery, or failure to disclose conflicts of interest concerning programs receiving federal funds.[58] Other espionage-related crimes that can be state espionage, depending on the details of the case, are conspiracy to kill nationals of the United States wherever they are in the world;[59] theft of government property;[60] transportation of ammunition without notice;[61] violations of the Arms Export Control Act and International Traffic in Arms Regulations (ITAR), including the export of defense articles without a permit;[62] and violations of the International Emergency Economic Powers Act, including laws that amend it.[63]

In this analysis, commercial espionage includes these crimes: economic espionage when a foreign government or government-supported firm benefits;[64] the conspiracy or actual theft of trade secrets for personal benefit, the benefit of a domestic entity, or a privately owned and operated foreign firm;[65] false, fictitious, or fraudulent claims made in the course of a commercial espionage investigation;[66] and the destruction of competitor trade secrets.[67] Other espionage-related crimes that could be state espionage or commercial espionage, depending on the details of the case, can include giving false statements in an espionage investigation;[68] wire fraud;[69] obstruction of justice;[70] destruction of evidence;[71] visa fraud discovered in the course of an espionage investigation;[72] smuggling;[73] bribery that involves a foreigner and is related to national defense;[74] and the filing of false tax returns that were uncovered in the course of an espionage investigation.[75]

Estimating the annual chance of a foreign-born or native-born individual committing espionage and being caught partly depends on the number of people in the United States who are foreign-born and native-born. This analysis estimates the annual chance by summing the resident population and the number of nonimmigrants who arrived from each country during the 1990–2019 period and dividing that sum by the number of individual spies. The same analysis is performed for native-born Americans without the nonimmigrant counts included because that does not apply to them.

Arms Export Control Act

Violations of the Arms Export Control Act (AECA) considerably complicate and lengthen this analysis. The AECA regulates the export of arms, ammunition, and some information about both to foreign governments, individuals, and entities.[76] One of the main goals of the act is to maintain the U.S. military's technological superiority over potential adversaries, according to government law enforcement officers tasked with enforcing such laws.[77] The U.S. immigration law considers the unlawful export of arms to be so akin to espionage that the same statute that designates spies as inadmissible aliens also designates violators of export-control laws such as the AECA to be inadmissible.[78] Out of the 1,485 spies identified in this analysis, 815, or 54.9 percent, of them violated the act.

"Out of the 1,485 spies identified in this analysis, 815, or 54.9 percent, of them violated the Arms Export Control Act."

> "281 of the 815 Arms Export Control Act violators benefited people in Mexico who were likely all part of drug cartels or engaged in other criminal activity."

In many cases, violations of the AECA are clearly related to espionage, as the intended beneficiary is, or is likely to be, a foreign government. One such example was the conviction of Chinese spy Kan Chen in 2016. He exported or attempted to export 180 export-controlled items to China, including 40 items that were sophisticated night-vision and thermal-imaging scopes used in military applications.[79] A second example is American-born John Reece Roth, who exported data on specialized plasma technology for use in drones that he had developed under a U.S. Air Force contract while a professor at the University of Tennessee.[80] Another case of an AECA violation that is clearly espionage is Mozaffar Khazaee, an Iranian-born U.S. citizen who attempted to export to Iran proprietary material about military jet engines and the U.S. Air Force's F-35 Joint Strike Fighter program that he had illegally gathered from his employer.[81]

However, many of these violations are not espionage-related, as the intended beneficiaries are likely private foreign purchasers, criminal organizations, rebel groups, or drug cartels unrelated to foreign governments. For instance, 281 of the 815 AECA violators benefited people in Mexico who were likely all part of drug cartels or engaged in other criminal activity. Of those 281 people, 170 were born in Mexico and 105 were native-born Americans. There are also many ambiguous cases, such as the 45 individuals who exported or attempted to export arms to Colombia and Venezuela to aid rebel groups, insurgencies, or (maybe) the governments there. Those individuals all violated the AECA, but it is unclear whether they are espionage-related in every instance.

Due to this ambiguity, and to avoid the problem of cherry-picking violators that could produce systematically biased results, this analysis counts all AECA violators as espionage and codes the country of benefit as the location of the beneficiaries, even if they are likely nongovernment entities.[82] For example, arms exports to FARC rebels in Colombia and Hezbollah in Lebanon are coded as benefiting Colombia and Lebanon, respectively.[83] Furthermore, this analysis codes AECA violations as state espionage when the export-prohibited items are stolen from the U.S. government or a contractor, and it codes AECA violations as commercial espionage when the violator legally purchases export-prohibited items in the United States with the intent to export them.

This analysis tries to take account of the ambiguity of AECA violators and how related they are to espionage in three different ways. First, the espionage is coded as "state espionage" in cases where the violators exported or attempted to export U.S. government property. In cases where the violators privately purchased arms that they exported or attempted to export without a permit, the espionage is coded as commercial espionage. However, this division is imperfect because AECA violators can steal government property for the aid of foreign governments or criminal organizations, as in the case of Colombian Luis Fernando Arcila-Giraldo, who attempted to purchase and export Stinger missiles to drug cartels in Colombia.[84] Second, this analysis also excludes all AECA violations in certain figures, tables, and analyses where noted. The Annex at https://infogram.com/annex-identified-spies-on-us-soil-1990-2019-1hd12y8p0rem4km?live includes the entire set of spies by espionage offense to allow readers to slice and dice the AECA convictions as they wish. Third, this analysis also shows that the number of AECA violators and the number of spies who committed non-AECA offenses are correlated. Thus, including the AECA numbers is less likely to skew the overall results, but they could still skew the country-of-origin information and generally inflate the number of spies.

Identifying Spies, Problems with Counting Spies, and Caution When Interpreting the Results

This analysis focuses on spies who have been identified by the government, following the methods of the Defense Personnel Security Research Center, by relying upon

publicly available information.[85] They are identified by being convicted of espionage or an espionage-related offense if they died after their discovery but before their conviction, or fled abroad after or before charges were filed against them. Their ethnicity is mainly assigned by their country of origin. If a spy's country of birth and ethnicity are different, that is reflected in the coding; for instance, Taiwan-born Ko-Suen Moo is of Korean ethnicity, so he is recorded as having been born in Taiwan and as ethnically Korean. The ethnicity of American-born spies is also recorded in broad categories including "white American," "black American," and "Hispanic American," where the specific ethnicity based on their family histories is unavailable. Specific ethnicities for native-born Americans are included if their ancestors' country of origin is known.

The sample of identified spies in this analysis could bear little resemblance to the population of total spies because of the secretive nature of espionage. Spies do not want to be caught and seek to conceal their illicit activities. This is unlike analyses of terrorists, who intend to make their crimes well known in order to inspire terror and trigger political or social reforms.[86] This might be less of a problem with amateur Chinese spies, especially those engaged in commercial espionage, because they are more likely to get caught than well-trained spies engaged in state espionage. Although this analysis seeks to build as comprehensive a list of spies as possible, some spies are undoubtedly unidentified, so this analysis could suffer from systematic undercounting of spies, espionage, and espionage-related crimes.

One problem that could lead to the undercounting of spies is that the government might not want to make known the individual spies that it identifies. Thus, the number of spies in this analysis could be undercounted because the government handles some espionage in secretive settings beyond the public view. However, if this does in fact happen, it likely involves few cases. The U.S. government does prosecute spies in court, and the DOJ typically issues press releases announcing when it has uncovered a spy and charged that person with a crime. The government even does this in some of the most embarrassing cases that expose significant government security failures. Furthermore, law enforcement and the DOJ have an incentive to publicize that they are capturing spies to act as a deterrent to other spies and to justify their budgets and investigative initiatives. The DOJ's China Initiative even takes credit for individuals convicted of espionage or espionage-related crimes if indictments against them were filed years prior to the initiative's creation, such as in the cases of Hao Zhang, Weiqiang Zhang, Ying Lin, and Xiang Haitao.[87] The DOJ would not announce its China Initiative and speak at prestigious conferences about it if it could *not* brag about how the program succeeds.[88]

Other government agencies could be more secretive in trying to uncover spies, but the FBI and other agencies charged with investigating espionage are mostly civil law enforcement agencies operating under the same incentives. Even when they cooperate with more secretive government agencies and don't publicize that cooperation, they publicize the indictments and prosecutions that result—as in the case of Edward Snowden.[89] Even if the DOJ's China Initiative was secret when it was started, it would only remain secret if it was a failure and didn't result in the identification or prosecution of any spies. It is tempting to ascribe a super-secretive identification and punishment process for spies beyond the public's view, especially in a culture rife with entertaining fiction about espionage, but the actual U.S. counterintelligence system is not set up that way to punish such offenders.

Overcounting of spies, espionage, and espionage-related crimes could also be a problem. Spies usually must be discovered and rarely announce their presence, so the discovery of spies is based on government and private-sector investigations of espionage. Political mandates to discover and prosecute spies could lead to an overidentification of spies. Mark Rasch, former computer-crime prosecutor, said, "If you're looking everywhere

"Political mandates to discover and prosecute spies could lead to an overidentification of spies."

> "The government also releases selective information about certain alleged spies without prosecuting them."

for spies, you will find spies everywhere, even where they don't exist."[90] For instance, prosecutors who are empowered and pushed to discover spies would likely result in marginal individuals being convicted of espionage-related crimes, such as making false statements or tax fraud, that were discovered in the course of an espionage investigation that wouldn't otherwise be prosecuted. In other cases, scientists in the United States may share data with scientists in foreign countries while collaborating on research projects that could result in the data being used as part of intelligence-gathering efforts by foreign governments. Those scientists in the United States who share the data could be spies, or they could just be scientists whose findings or data are used as a source of intelligence—but these marginal individuals are included in this analysis if they're prosecuted for espionage or espionage-related crime.

Prosecutors might also entirely ignore spies from friendly foreign powers. For instance, spying by Israel in the mid-1990s was rarely prosecuted, but the government claims that it was likely significant.[91] Commercial espionage conducted by the French government is also a big problem, according to former defense secretary Robert Gates.[92] Spies from those countries could either be deported from the United States; forced out by other means, such as diplomatic pressure on the foreign government to recall them; given stern warnings to stop; or be entirely ignored because the foreign government is not considered a threat to the United States. This source of bias would result in a relative undercounting of spies from friendly countries and a relative overcounting of spies from less-friendly countries.

In still other cases, individuals could be accused of espionage based on unfounded allegations, investigated or charged with crimes, convicted, and then cleared, as in the case of Russian-born Sergey Aleynikov. He was convicted of theft of trade secrets and another related offense and sentenced to eight years in prison. The Federal Court of Appeals unanimously reversed his conviction and entered a judgment of acquittal.[93] Aleynikov was lucky, and his counsel was especially competent, but some people convicted of espionage or espionage-related crimes are likely innocent and are either waiting for their convictions to be overturned or else they will continue to languish in prison for crimes they didn't commit.

Another problem is the selectiveness of government espionage and espionage-related prosecutions. For instance, there are many leakers of classified information, and very few of them are prosecuted. When they are investigated and prosecuted, political and policy reasons are likely the paramount justifications rather than a commitment to enforcing the law.[94] The government also releases selective information about certain alleged spies without prosecuting them. The government did this in the case of Chinese-born entrepreneur Liu Ruopeng, who earned his masters and doctorate degrees from Duke University and allegedly turned over research secrets to the Chinese government while using stolen research to start a successful firm in China.[95] Despite the serious allegations and convincing evidence that was leaked to the public, the government did not charge Ruopeng with any crimes, which indicates that the government likely selectively released evidence to show Ruopeng in the worst light.

Government efforts to identify spies from China, a new focus on commercial espionage, or other initiatives could boost the number of prosecutions and convictions but reduce them elsewhere. In other words, spies will always exist, but the spies that are identified are those that the government targets. If the government directs law enforcement resources to targeting Chinese spies, then it could relax efforts to identify Iranian or Russian spies, for instance. Government targeting is based on political and administrative objectives that might be related to the changing nature of espionage or could be reactive to other political or administrative considerations.

The sample of spies in this analysis could be too small and undercounted, too large and overcounted, or systematically skewed because of the selective nature of government

prosecutions. Thus, the sample of spies in this analysis could be biased and unrepresentative of the total population of spies in the United States—a phenomenon called sampling bias. In short, sampling bias in this analysis could mean that the identified spies here could differ to a statistically significant extent from the total population of spies. They could come from different countries, spy for different countries, or commit different crimes. It is tempting to use this analysis to cherry-pick marginal cases to include those who probably should be charged with espionage and to exclude those who probably shouldn't have been, but that would introduce an entirely new layer of bias that would significantly reduce the utility of this analysis. As a result, this analysis includes the widest possible sample without cherry-picking individual spies for inclusion or exclusion. Regardless, one must keep the above problems in mind when considering the findings of this analysis.

The government's intense public focus on espionage and espionage-related crimes, growing media and public scrutiny of espionage, the building geopolitical and economic conflict with China, and the lack of any thorough account of all espionage and espionage-related crimes justify this analysis. Regardless of the above problems with identifying spies, this analysis is a first step in analyzing the totality of espionage and espionage-related crime in the United States. Systematic efforts like this to build a dataset will help identify whether a problem exists, the scale of the problem, and characteristics of the problem far better than a few anecdotes selectively used in public statements. The main hope is that this analysis will help answer those questions. The secondary hope is this analysis will inspire other researchers who will take the data here, add to it, refine the methods, and produce better research in the future.

Sources

The identities of spies, details of their crimes, and other information come from numerous data sets, documents, and other sources. Government agencies have an incentive to publicize the identification of spies to highlight the threat posed by espionage and to justify their enforcement activities. The main source for state espionage is a series of reports published by the Defense Personnel and Security Research Center Office of People Analytics.[96] The office's impressive studies include the identities and other biographical information of spies who committed espionage against the U.S. government from 1947 to 2015.

The first source for commercial espionage is a database of all known prosecutions of economic espionage and theft of trade secret cases under or related to the Economic Espionage Act since its enactment in 1996.[97] This information is compiled by Jeremy Wu, a retired senior adviser at the U.S. Census Bureau.[98] The second source is a public comment filed by the Federal Public Defender in the Southern District of Texas in 2013.[99] The third source is a paper written by attorney Thomas J. Nolan that includes a list of 137 different economic espionage and trade theft prosecutions, many of which were included in the database compiled by Wu.[100] The fourth source is a *Cardozo Law Review* article written by Andrew Chongseh Kim that also heavily relies upon Wu's data.[101]

Many sources supplied information on both state espionage and commercial espionage. The first is a report from the Australian Strategic Policy Institute that has an appendix listing some Chinese spies.[102] The second source is the U.S. Department of State's list of people barred from exporting weapons because of violations of the AECA and the International Traffic in Arms Regulations.[103] The third is the *Federal Register*, which publishes the names of those people barred from exporting arms, as well as other information about them.[104] The fourth is a list of cases published by the U.S. Department of Commerce, Bureau of Industry and Security, and accompanying information.[105] The fifth are DOJ press releases dating back to July 1994 and DOJ reports and fact sheets on export violations, espionage, and other violations of espionage-related laws.[106] The sixth are Immigration and Customs Enforcement press releases on counter-proliferation enforcement

"This analysis includes the widest possible sample without cherry-picking individual spies for inclusion or exclusion."

> "The 184 Chinese-born spies accounted for 12.4 percent of all identified spies."

actions and removals.[107] The seventh are press releases published by the Bureau of Diplomatic Security.[108]The eighth are thousands of news stories, indictments, and fact sheets compiled by researchers that are all available upon request.[109]

Data on the population of the United States, the annual number of residents from each country of origin, and the annual number of admissions from each country come from the U.S. Census, the American Community Survey, and the Department of Homeland Security, respectively.[110]

ESPIONAGE

This analysis identifies 1,485 known spies who committed espionage or espionage-related crimes in the United States from January 1, 1990, to the end of 2019. Of those spies, 890 were foreign-born, 583 were native-born Americans, and 12 were of unknown origins (see Table 1).

From 1990 through 2019, the approximate annual chance that somebody on U.S. soil committed espionage or an espionage-related crime, and was identified doing so, was about 1 in 6.5 million (see Table 1). The chance that a foreign-born person committed espionage or an espionage-related crime and was identified doing so was about 1 in 2.2 million per year during the same period. Foreign-born spies accounted for 59.9 percent of all spies from 1990 to 2019. The chance that a native-born American committed espionage or an espionage-related crime and was identified was about 1 in 13.1 million per year from 1990 to 2019. Native-born American spies accounted for 39.3 percent of all spies during that time. Figure 1 shows the global distribution of all spies on U.S. soil by their countries of origin from 1990 to 2019.

The 184 Chinese-born spies accounted for 12.4 percent of all identified spies during this time (see Table 1). Given the population of Chinese-born immigrants and nonimmigrant admissions from China, Chinese-born spies were 16 times more likely to be identified spies than their percentage of the population would suggest (see Figure 2).[111] This is higher than for all foreign-born spies, who were about 2.9 times as likely to be spies as their percentage of the population would suggest. By contrast, native-born American spies were underrepresented because they were 39.3 percent of all spies, yet 79.3 percent of the population. Using this metric, Chinese-born spies were the 13th most overrepresented group of spies by national origin in the United States (see Figure 2).

Figure 3 shows the number of identified spies over time by select origins. The total number of identified spies has shrunk from an annual high of 119 in 2011 to 49 in 2019. Only 17 Chinese-born spies were identified from 1990 to 2003, while 167, almost 10 times as many, were identified from 2004 to 2019, for an average of about 10.5 Chinese-born spies identified per year during the latter period. Chinese-born spies accounted for 14.1 percent of all identified spies since 2004. During the same time, American-born spies accounted for 35.9 percent of all identified spies.

As previously mentioned, counting violators of the AECA increases the number of spies because the violators account for 54.9 percent of the total and may skew the espionage data. The number of AECA violators and non-AECA spies is positively correlated with a coefficient of 0.63, meaning that their numbers generally move in the same direction (see Figures 3 and 4). Even with the AECA violators excluded, the number of identified spies still increases in a pattern very similar to that of all identified spies (see Figure 4). Table 2 presents identified spies on U.S. soil by selected countries of origin, excluding all AECA violators. Although their numbers drop, the percentage of Chinese and American spies increases when the AECA is excluded. Mexico, Venezuela, and Lebanon drop out of the top-10 list of foreign countries that send spies because most violated the AECA. Iraq, Vietnam, and Cuba rise to take their place.

The annual chance of being an identified spy drops for many countries on the list when the AECA isn't included (see Table 2). The annual chance of a native-born American becoming an

Table 1

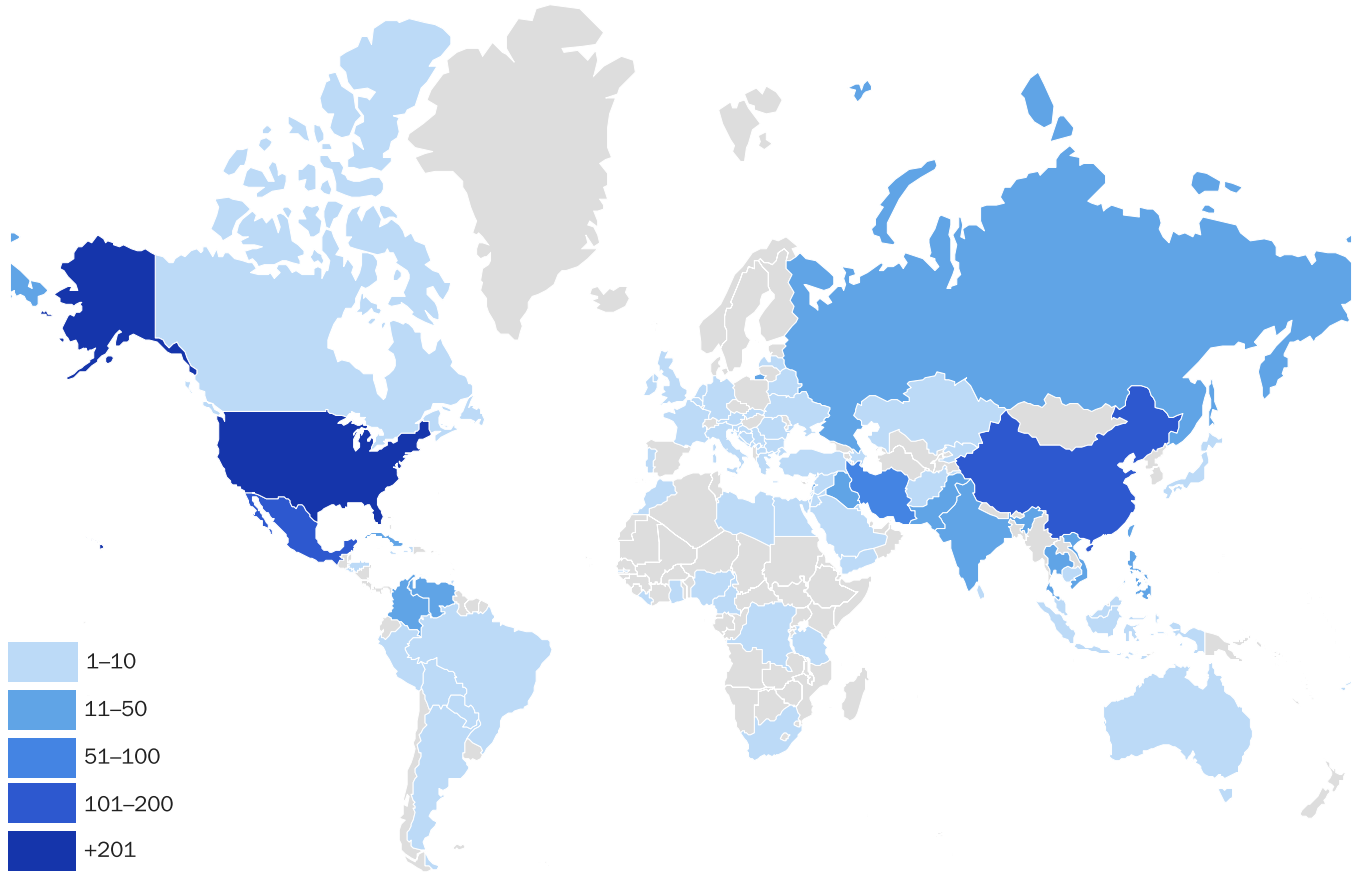
Identified spies on U.S. soil by country of origin for top 10 foreign countries and the United States, 1990–2019

Country or citizenship of birth	Spies	Percentage of all spies	Annual chance of being an identified spy
All	1,485	100%	1 in 6,476,337
All foreign-born	890	59.9%	1 in 2,240,123
United States	583	39.3%	1 in 13,076,588
China	184	12.4%	1 in 403,589
Mexico	172	11.6%	1 in 3,196,850
Iran	84	5.7%	1 in 119,917
Taiwan	41	2.8%	1 in 516,671
Russia	35	2.4%	1 in 499,007
India	26	1.8%	1 in 2,734,624
Pakistan	23	1.5%	1 in 431,219
Venezuela	23	1.5%	1 in 900,069
Lebanon	20	1.3%	1 in 218,809
South Korea	17	1.1%	1 in 2,143,968

Sources: See Methodology section; author's calculations.

Figure 1

Spies by their country of origin, 1990–2019



Source: See Methodology section.

Figure 2

Over- and underrepresentation of spies as a percentage of their U.S. population, 1990–2019

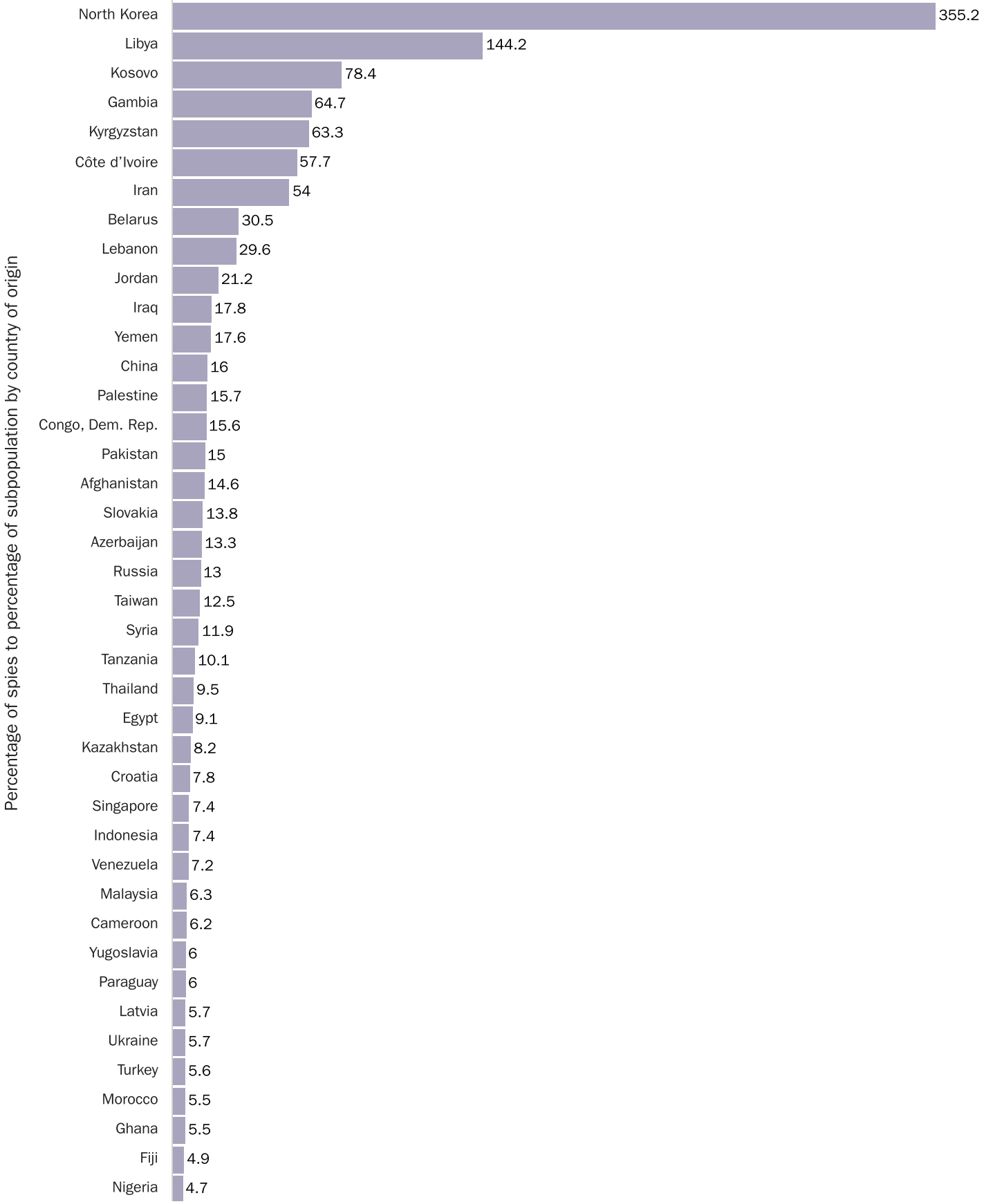
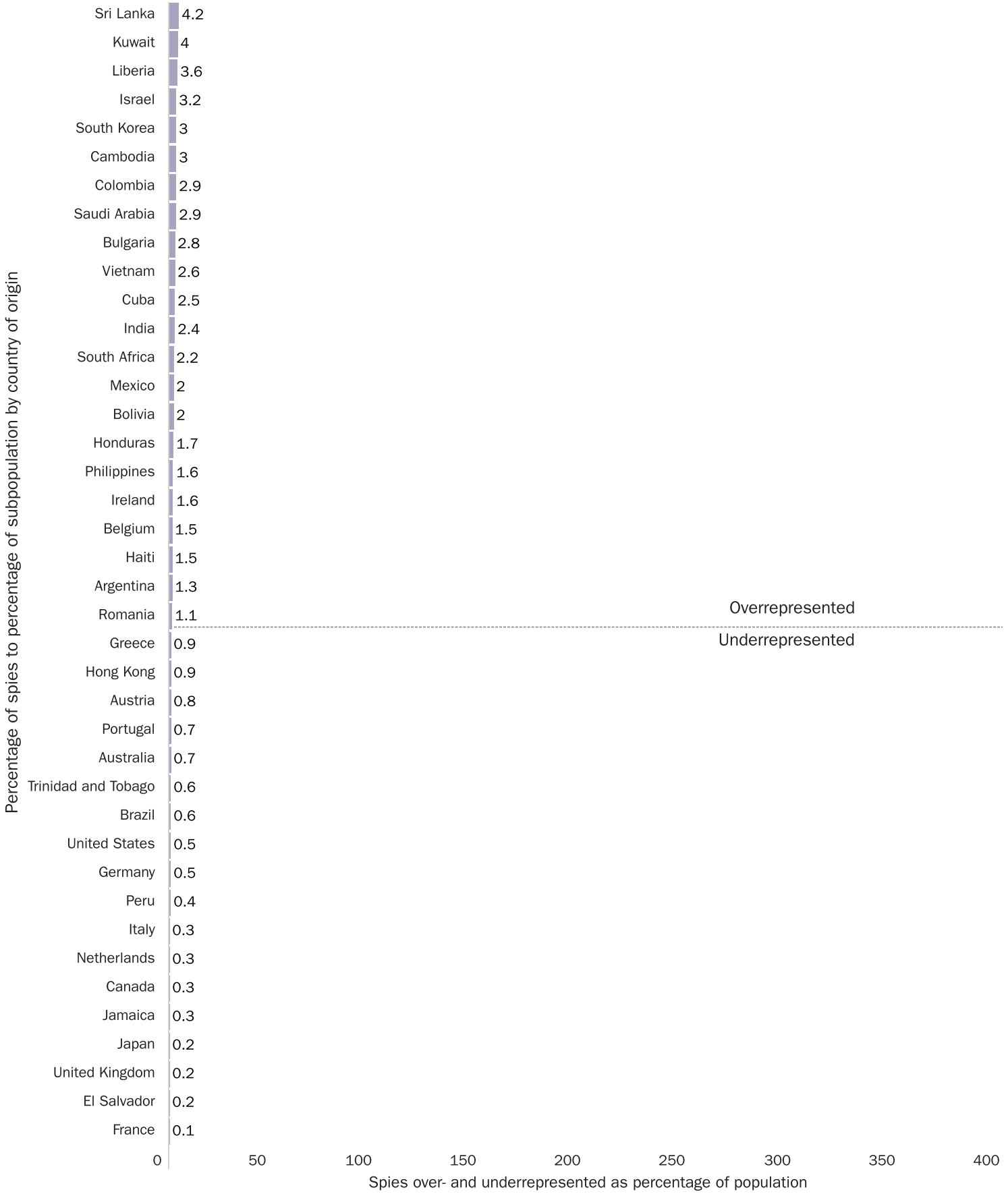


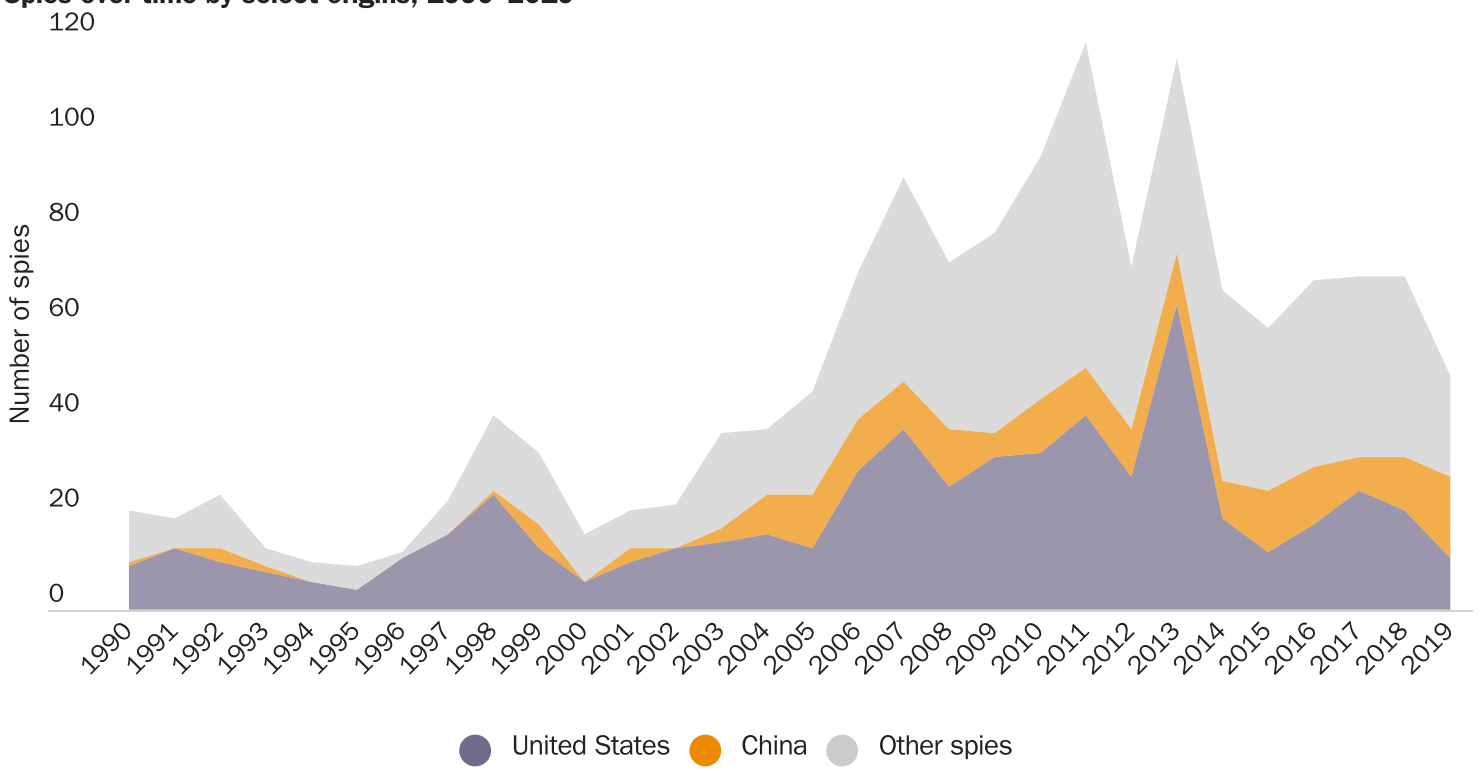
Figure 2 (continued)



Sources: See Methodology section; author's calculations.

Figure 3

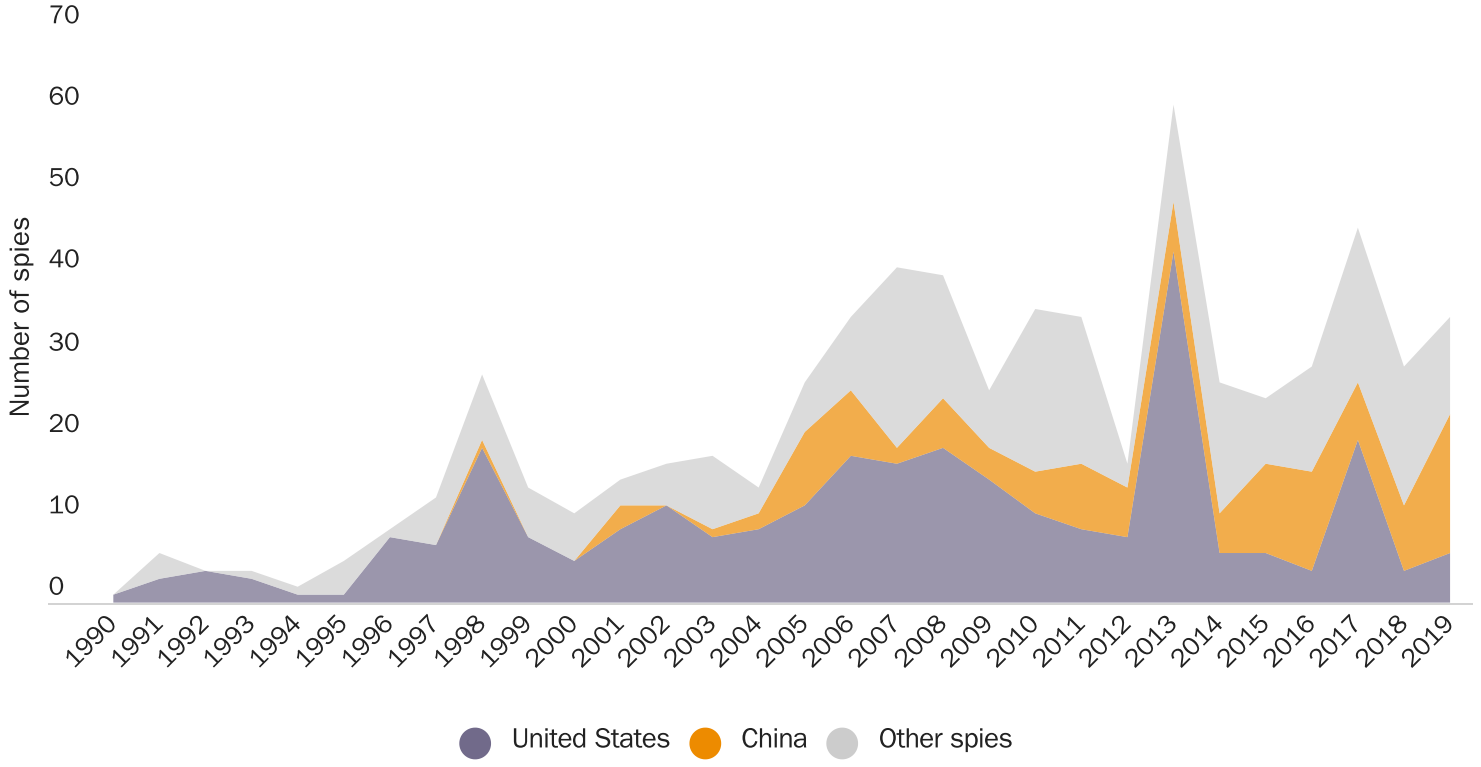
Spies over time by select origins, 1990–2019



Source: See Methodology section.

Figure 4

Spies over time by select countries of origin, excluding AECA violators, 1990–2019



Source: See Methodology section.
Note: AECA = Arms Export Control Act.

Table 2

Identified spies on U.S. soil by country of origin for top 10 foreign countries and Americans, excluding AECA violators, 1990–2019

Country or citizenship of birth	Spies	Percentage of all spies	Annual chance of being a known spy
All	670	100%	1 in 14,354,270
All foreign-born	374	55.8%	1 in 5,330,775
United States	296	44.2%	1 in 25,755,578
China	121	18.1%	1 in 613,723
Iran	60	9.0%	1 in 167,884
Taiwan	27	4.0%	1 in 784,575
Russia	19	2.8%	1 in 919,223
India	14	2.1%	1 in 5,078,587
Cuba	12	1.8%	1 in 2,561,522
Pakistan	9	1.3%	1 in 1,102,005
South Korea	9	1.3%	1 in 4,049,718
Iraq	8	1.2%	1 in 500,487
Vietnam	7	1.0%	1 in 4,702,091

Sources: See Methodology section; author's calculations.
Note: AECA = Arms Export Control Act.

identified spy drops to about 1 in 25.8 million, and for Chinese-born spies it drops to 1 in 613,723 when AECA violators are excluded. Iranians remain the most likely to become identified spies, followed by Iraqis and then Chinese (see Table 2). In the expanded list that includes all countries, a Chinese-born person on U.S. soil has the ninth-highest annual chance of being an identified spy compared to people from other countries.

Spies don't just spy for their countries of birth. Table 3 displays the main countries that benefited from espionage by the number of spies. Columns 2 and 3 in Table 3 include all espionage, and columns 5 and 6 exclude violators of the AECA. For all espionage, Mexico was the main beneficiary, with 19 percent of all spies on U.S. soil spying on behalf of Mexico or people in Mexico, mostly via violations of the AECA. Of the 282 spies for Mexico or the benefit of Mexicans, 111 (39.4 percent) were not from Mexico. China is the second-largest beneficiary of espionage on U.S. soil, with 18.6 percent of the total. Of the 276 spies for China, 111 (37.6 percent) were not born in China, and 65 were native-born Americans.

When the AECA is excluded, spying on behalf of Mexico virtually disappears, and espionage for personal benefit tops the list at 26.4 percent of spies (see Table 3). This primarily includes native-born Americans and foreign-born people who stole trade secrets to build domestic businesses or to make money in an illicit deal and whistleblowers who exposed government secrets for idealistic reasons. One example of the latter is Matthew Diaz, a former active-duty lieutenant commander in the U.S. Navy, who mailed classified information to a nonprofit organization to expose unconstitutional practices at Guantanamo Bay.[112] After personal benefit inside the United States, China becomes the second main beneficiary of spying in the United States and accounts for 26.1 percent of all spies when the AECA violators are excluded (see Table 3).

Figure 5 is a map showing the top countries by the number of spies spying for them for all forms of espionage, including violations of the AECA. Figure 6 is a map with the main countries that benefit by the number of spies spying for them that excludes violators of the AECA.

> "When the Arms Export Control Act is excluded, spying on behalf of Mexico virtually disappears."

Table 3

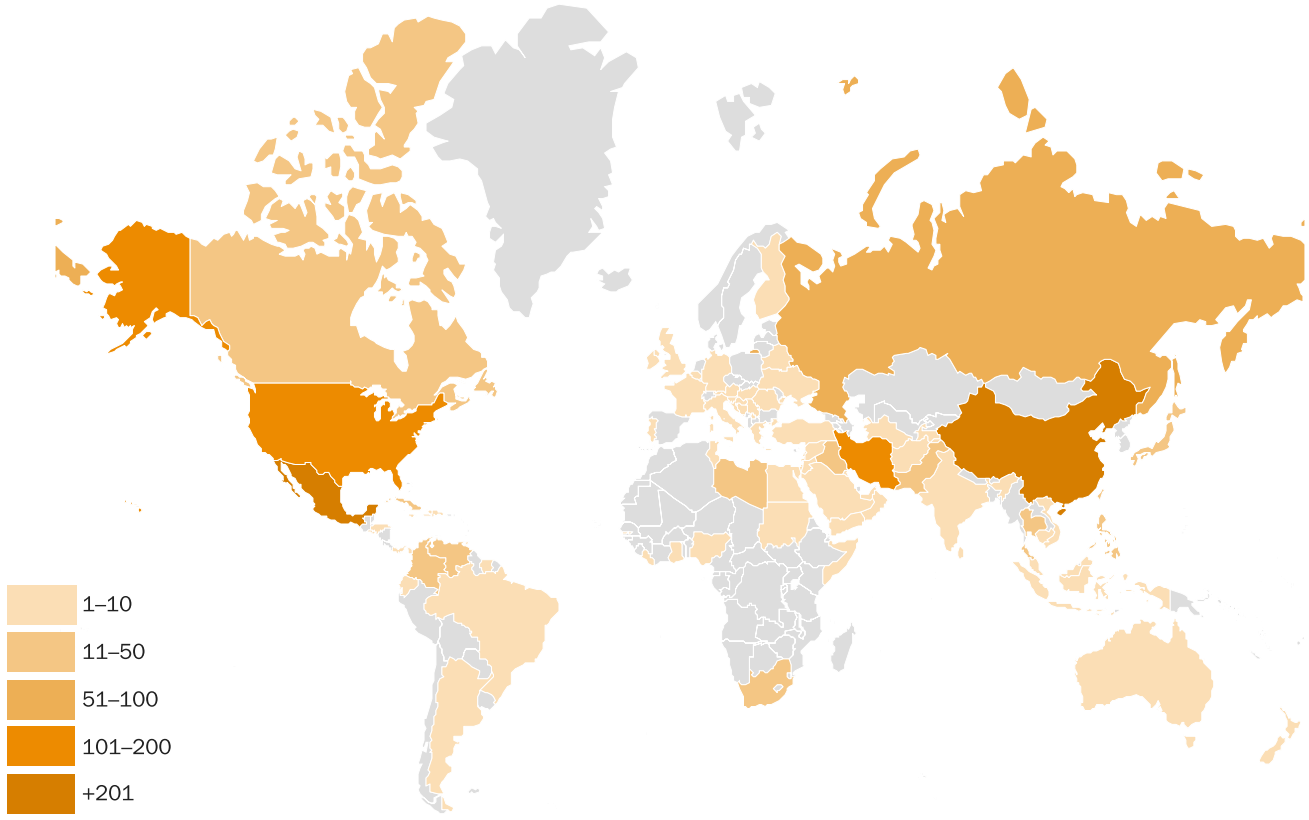
Identified spies on U.S. soil by main country of benefit for top 10 foreign countries and the United States, 1990–2019

Main country of benefit	All spies	Percentage of all spies	Main country of benefit	Spies, AECA excluded	Percentage of all spies, AECA excluded
All	1,485	100%	All	670	100%
Mexico	282	19.0%	United States	177	26.4%
China	276	18.6%	China	175	26.1%
United States	177	11.9%	Iran	85	12.7%
Iran	149	10.0%	Russia	35	5.2%
Russia	57	3.8%	Cuba	24	3.6%
Venezuela	37	2.5%	Iraq	20	3.0%
Iraq	34	2.3%	Taiwan	14	2.1%
Unknown	33	2.2%	Unknown	11	1.6%
Cuba	24	1.6%	Pakistan	11	1.6%
Pakistan	22	1.5%	South Korea	10	1.5%
Lebanon	21	1.4%	Libya	8	1.2%

Sources: See Methodology section; author's calculations.
Note: AECA = Arms Export Control Act.

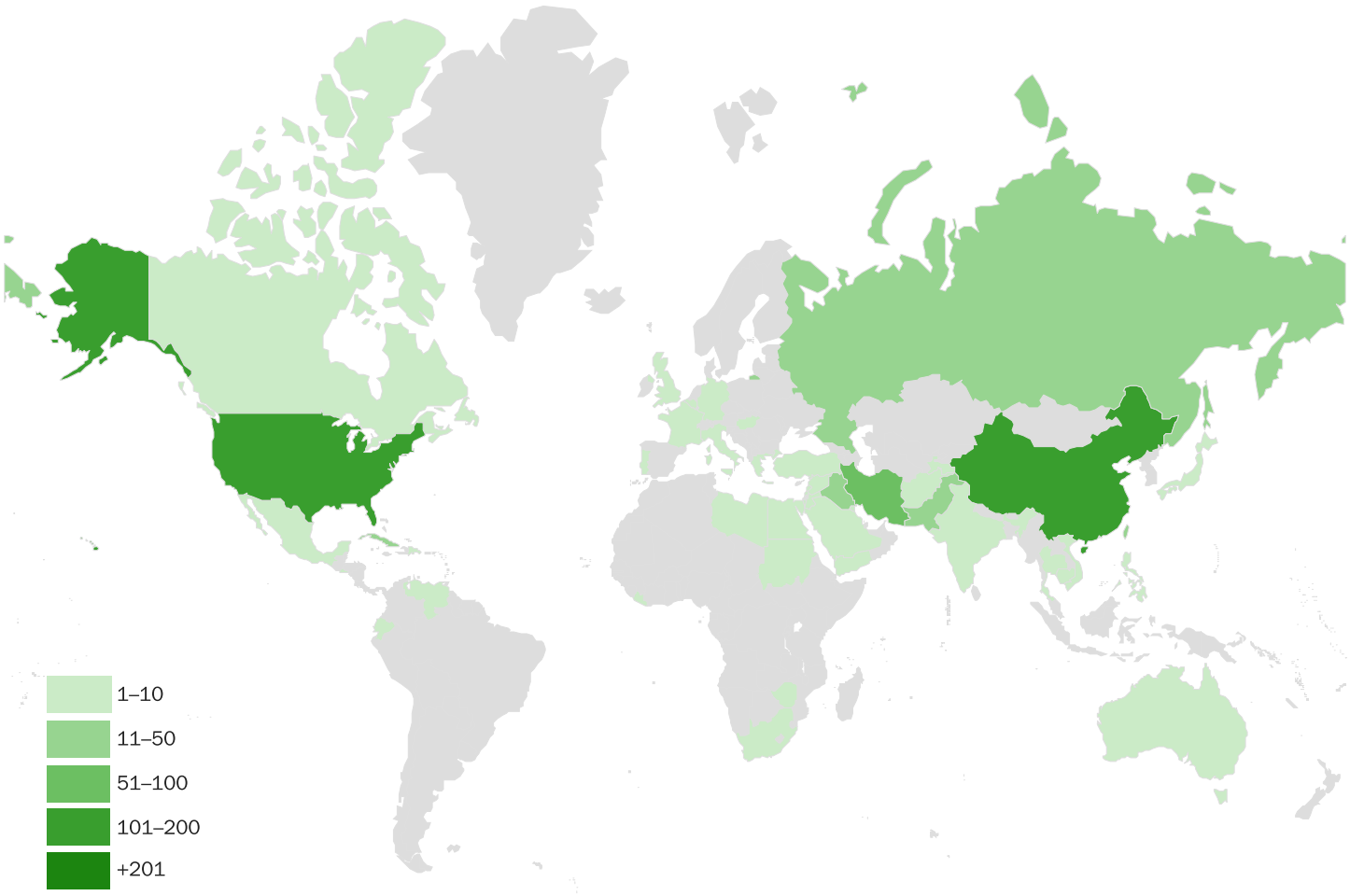
Figure 5

Spies by the main country of benefit, 1990–2019



Source: See Methodology section.
Notes: Al Qaeda is excluded as a main country of benefit; East Germany and Germany are combined; the Soviet Union is combined with Russia; Europe and Eastern Europe are excluded as countries; unknown countries of origin are excluded; and "personal gain" is recoded as a benefit to the United States.

Figure 6
Spies by the main country of benefit, excluding AECA violators, 1990–2019



Source: See Methodology section.
Notes: Al Qaeda is excluded as a main country of benefit; East Germany and Germany are combined; the Soviet Union is combined with Russia; Europe and Eastern Europe are excluded as countries; unknown countries of origin are excluded; and "personal gain" is recoded as a benefit to the United States.
AECA = Arms Export Control Act.

Table 4 shows the ethnicity of identified spies for the top 10 ethnicities, regardless of their country of birth or citizenship. White Americans account for 30.3 percent of all identified spies, followed by 12.9 percent who are ethnically Chinese.

Assistant Attorney General for National Security John C. Demers stated that there is a persistent effort by the Chinese government to recruit American-born spies who are of Chinese descent.[113] Comparing the countries of origin for spies in Table 1 to the ethnicity of spies in Table 4 shows that only eight spies of Chinese ancestry who were not born in China committed espionage in the United States. Thus, only 4.2 percent of spies of Chinese ethnicity were not born in China. Of those eight non-China-born spies of Chinese ethnicity, five were born in the United States, and one each came from Singapore, Malaysia, and Hong Kong. Native-born Americans who are ethnically Chinese are about 1.1 percent of the U.S. population and about 0.9 percent of all native-born American spies, so they are slightly underrepresented as spies.[114]

Comparing the spies who spied for China in Table 3 with the ethnicity of spies in Table 4 reveals a vastly different picture. Ninety-nine of the 276 spies who spied for China, or 35.8 percent, were not ethnically Chinese. For instance, 58 were native-born white Americans, 19 were Taiwanese, 5 were Indian, 4 were Korean, 2 were

> "Native-born Americans who are ethnically Chinese are about 0.9 percent of all native-born American spies."

Vietnamese, and 2 were Pakistani. There was one spy of each of the following ethnicities who spied for China: Fijian, Filipino, Ghanaian, Hispanic American, Iranian, Israeli, Jordanian, Malaysian, and Nigerian.

Table 5 shows the number of spies who engaged in state or commercial espionage. As previously mentioned, state espionage is the act of obtaining information or items that are not publicly available from the U.S. government in the interests of a foreign government or in service of a broader ideological goal. Commercial espionage is the act of unlawfully and clandestinely obtaining valuable proprietary

Table 4

Identified spies on U.S. soil by ethnicity for top 10 ethnicities, 1990–2019

Ethnicity	All spies	Percentage of all spies
All	1,485	100%
White American	450	30.3%
Chinese	192	12.9%
Mexican	172	11.6%
Hispanic American	92	6.2%
Iranian	86	5.8%
Taiwanese	40	2.7%
Russian	35	2.4%
Indian	27	1.8%
Pakistani	23	1.5%
Korean	22	1.5%

Sources: See Methodology section; author's calculations.

Table 5

Identified spies on U.S. soil by country of origin for top 10 foreign countries and the United States, 1990–2019

Country or citizenship of birth	Commercial	Country or citizenship of birth	Commercial, AECA excluded	Country or citizenship of birth	State	Country or citizenship of birth	State, AECA excluded
All	1,083	All	396	All	402	All	274
All foreign-born	686	All foreign-born	239	All foreign-born	216	All foreign-born	135
United States	397	United States	157	United States	186	United States	139
Mexico	172	China	85	China	61	China	36
China	123	Iran	52	Russia	24	Russia	15
Iran	74	Taiwan	18	Taiwan	14	Taiwan	9
Taiwan	27	India	9	India	11	Cuba	9
Pakistan	18	Vietnam	6	Iran	10	Iran	8
Lebanon	18	Pakistan	5	Cuba	9	Venezuela	6
Venezuela	17	South Korea	5	South Korea	8	Iraq	6
India	15	Colombia	4	Egypt	7	India	5
Unknown	12	Russia	4	Venezuela	6	Egypt	5
Russia	11	Canada	3	Iraq	6	South Korea	4

Sources: See methodology section; author's calculations.
Note: AECA = Arms Export Control Act.

information; intellectual or other property; or financial, trade, or economic information from U.S. firms, establishments, or persons, for one's personal benefit or the benefit of another domestic firm, foreign firm, foreign government, or other foreign or domestic entity. Violations of the AECA count as state espionage when the export-prohibited arms and equipment are state-owned and likely stolen. Violations of the AECA are counted as commercial espionage when the export-prohibited items were acquired legally prior to the attempted or actual unlawful export.

For all identified spies, 27.1 percent engaged in state espionage and the remaining 72.9 percent engaged in commercial espionage (see the whole numbers in Table 5). When AECA violators are excluded, 41.1 percent of spies engaged in state espionage and 58.9 percent engaged in commercial espionage (see Table 5). Table 5 contains four different columns of espionage by broad type that both include and exclude the AECA, for a total of 44 country-of-origin cells. Only 18 countries are represented in those 44 cells. In each column, the percentage of total spies coming from the United States and 10 other countries accounts for between 81.6 percent and 88.3 percent of all spies.

Table 6 shows identified spies by the country that they spied for and whether those countries benefited from state or commercial espionage. As in earlier tables, if the spy was an American spying for personal gain, then his espionage is counted as benefiting the United States. Again, the countries that the individuals spied for are highly concentrated among a few top offenders. For instance, the top 10 foreign countries and the United States account for 93.1 percent of commercial espionage when the AECA is excluded (see the whole numbers in Table 6, column 4). The lowest percentage accounted for among the top 10 countries and the United States is for state espionage including AECA violators, and that was still 74.1 percent (see the whole numbers in Table 6, column 6). There is a significant overlap between the countries included in both Table 5 and Table 6.

Table 7 shows the most serious espionage or espionage-related crime that spies committed, or are charged with committing,

> "27.1 percent of spies engaged in state espionage, and the remaining 72.9 percent engaged in commercial espionage."

Table 6

Identified spies on U.S. soil by the country of benefit for the top 10 foreign countries of benefit and the United States, 1990–2019

Country of benefit	Commercial	Country of benefit	Commercial, AECA excluded	Country of benefit	State	Country of benefit	State, AECA excluded
All	1,083	All	396	All	402	All	274
Mexico	282	United States	122	China	111	China	66
China	165	China	109	United States	55	United States	55
Iran	136	Iran	77	Russia	41	Russia	27
United States	122	Iraq	10	Cuba	19	Cuba	19
Venezuela	29	Taiwan	10	Iraq	14	Unknown	11
Unknown	22	Russia	8	Iran	13	Iraq	10
Iraq	20	Libya	8	Unknown	11	Iran	8
Lebanon	19	Pakistan	7	Japan	11	Venezuela	8
Pakistan	18	Syria	7	Venezuela	8	Soviet Union	7
Russia	16	South Korea	6	South Korea	8	Afghanistan	6
Taiwan	15	Cuba	5	Philippines	7	Taiwan	4

Sources: See Methodology section; author's calculations.

Note: AECA = Arms Export Control Act.

prior to trial if their trial hasn't occurred yet. Violations of the Arms Export Act dominate the list, with 54.9 percent of the total. The next most common is violations of the International Emergency Economic Powers Act, which largely covers trading with nations that the president of the United States has embargoed. The third and fourth most common crimes are theft of trade secrets and economic espionage. Theft of trade secrets accounts for 7.5 percent of espionage or espionage-related crimes, followed by the related crime of economic espionage, which accounts for 6.9 percent. Crimes related to economic espionage and theft of trade secrets, including conspiracy and destruction of competitor trade secrets, are a major focus of the DOJ's China Initiative. However, those types

Table 7

All spies by their most serious espionage or espionage-related crime, 1990–2019

Most serious espionage-related crime	Crimes	Percentage
Agent of a foreign government	72	4.8%
Arms Export Control Act	815	54.9%
Atomic Energy Act	3	0.2%
Bribery	35	2.4%
Conspiracy to defraud the United States	11	0.7%
Conspiracy to steal trade secrets	26	1.8%
Destruction of competitor trade secrets	1	0.1%
Economic espionage	102	6.9%
Espionage	4	0.3%
False statements	26	1.8%
False, fictitious, or fraudulent claims	3	0.2%
Filing false tax return	1	0.1%
Gathering or delivering defense information to aid a foreign government	46	3.1%
International Emergency Economic Powers Act	136	9.2%
Intelligence Identities Protection Act	1	0.1%
Obstruction of justice	1	0.1%
Photographing or sketching defense installations	2	0.1%
Produce nuclear materials outside the United States	2	0.1%
Smuggling	24	1.5%
Theft of government property	7	0.5%
Theft of trade secrets	111	7.5%
Theft, bribery, failure to disclose conflicts of interest concerning programs receiving federal funds	3	0.2%
Unauthorized access to a computer	6	0.4%
Unauthorized removal and retention of classified documents or material	1	0.1%
Unlawful retention/communication of national defense information	40	2.7%
Visa fraud	1	0.1%
Wire fraud	5	0.3%
Total	1,485	100%

Source: See Methodology section.

of crimes only account for 16.3 percent of all espionage or espionage-related crimes.[115]

Table 8 shows the broad victims of espionage conducted on U.S. soil. The government is the major victim, even in cases where the AECA is excluded. American firms are the second most common victim, followed distantly by hospitals and universities.

Chinese Espionage

Chinese espionage is the main concern today and the justification for the DOJ's China Initiative.[116] This subsection specifically examines the dynamics of Chinese espionage, both in total and in the prosecutions claimed by the initiative up through the end of 2019. Of all identified spies, 184, or 12.4 percent, were born in China (see Table 9). There were 192 total ethnic Chinese spies identified, of whom 5, or 2.6 percent, were native-born Americans. In other words, 97.4 percent of ethnic Chinese spies were *not* born in the United States. Of ethnic Chinese spies born abroad, 98.4 percent were born in China. Excluding violations of the AECA lowers the number of spies spying for China from 184 to 121, a reduction of 34.2 percent. That reduces the number of spies guilty of state espionage by 41 percent and the number guilty of commercial economic espionage by 30.9 percent.

Overall, 276 individuals in the database spied for China, which means that they account for about 18.6 percent of all spies identified from 1990 to 2019. Thus, 66.7 percent of all spies for China were born in China, and 67.8 percent of all spies for China were ethnically Chinese. In other words, about a third of all spies for China were not from China or ethnically Chinese.

Table 10 shows the specific countries of origin for spies who spied for China. Those born in China account for 62 percent of the total, followed by native-born American spies, with 23.6 percent. When AECA violators are excluded, the percentages are very similar: 64 percent for China-born spies and 24 percent for native-born Americans.

Figure 7 shows the yearly numbers of spies from China and places other than China who committed the crimes of economic espionage, theft of trade secrets, and conspiracy to steal trade secrets. Prosecutions for these crimes began in 1996, the year that Congress passed the Economic Espionage Act. The identified number of spies from China increases over the period; the annual number is roughly constant from 2010 on and accounts for half of all spies who committed the crimes of economic espionage, theft of trade secrets, and conspiracy to steal trade secrets.

The DOJ created its China Initiative in 2018 to focus on detecting, prosecuting, and stopping Chinese espionage, with a particular focus on impeding commercial espionage.[117] The DOJ's China Initiative takes credit for many prosecutions, including many that began before the initiative started. Of the 30 individuals identified and prosecuted by the DOJ as part of its initiative, 21 were born in China, 4 were born in Taiwan, 1 was born in Hong Kong, and 4 were born in the United States (see Table 11). All four native-born Americans were white and not of Chinese ethnicity. The first was James Patrick Lewis, a former professor at West Virginia

> "67.8 percent of all spies for China were ethnically Chinese."

Table 8

Broad victims of espionage carried out on U.S. soil, 1990–2019

Victim	Identified spies	Percentage	Spies, AECA excluded	Percentage
U.S. government	1,237	83.3%	424	63.3%
U.S. firms	242	16.3%	240	35.8%
U.S. hospitals	2	0.1%	2	0.3%
U.S. universities	4	0.3%	4	0.6%
All	1,485	100%	670	100%

Source: See Methodology section.

Table 9

Chinese espionage in the United States, 1990–2019

	All spies	All spies, AECA excluded	State espionage	State espionage, AECA excluded	Commercial espionage	Commercial espionage, AECA excluded
China-born spies	***184***	***121***	***61***	***36***	***123***	***85***
Ethnic Chinese spies	*192*	*127*	*63*	*37*	*129*	*90*
Ethnic Chinese, foreign-born*	187	124	62	37	125	87
Ethnic Chinese, China-born	184	121	61	36	123	85
Ethnic Chinese, native-born United States	5	3	1	0	4	3
Ethnic Chinese, born outside China or the United States	3	3	1	1	2	2
China is country of benefit	*276*	*175*	*111*	*66*	*165*	*109*
Ethnic Chinese, foreign-born*	173	114	58	34	115	80
Ethnic Chinese, China-born	171	112	57	33	114	79
Ethnic Chinese, native-born United States	4	3	0	0	4	3
Ethnic Chinese, born outside China or the United States	2	2	1	1	1	1

Source: See Methodology section.
Note: AECA = Arms Export Control Act.
*Includes ethnic Chinese, China-born spies.

University, who was convicted of not disclosing a conflict of interest with a Chinese university when he received federal research funds.[118] The second was Ron Rockwell Hansen, a former Defense Intelligence Agency officer who attempted to transmit national defense information to China.[119] The third was Kevin Patrick Mallory, a former Central Intelligence Agency officer who also tried to transmit national defense information to a Chinese agent.[120] The last was Candace Marie Claiborne, a former U.S. Department of State employee who tried to defraud the United States by selling secrets to the Chinese.[121] Mallory and Hansen were retired when they began spying for China and used either retained documents from when they were employed or attempted to gather classified information from contacts who worked with their former employers.[122] Claiborne was still employed by the Department of State when she became a spy.[123] Table 11 does not include the cases of hackers or individuals residing abroad

Table 10

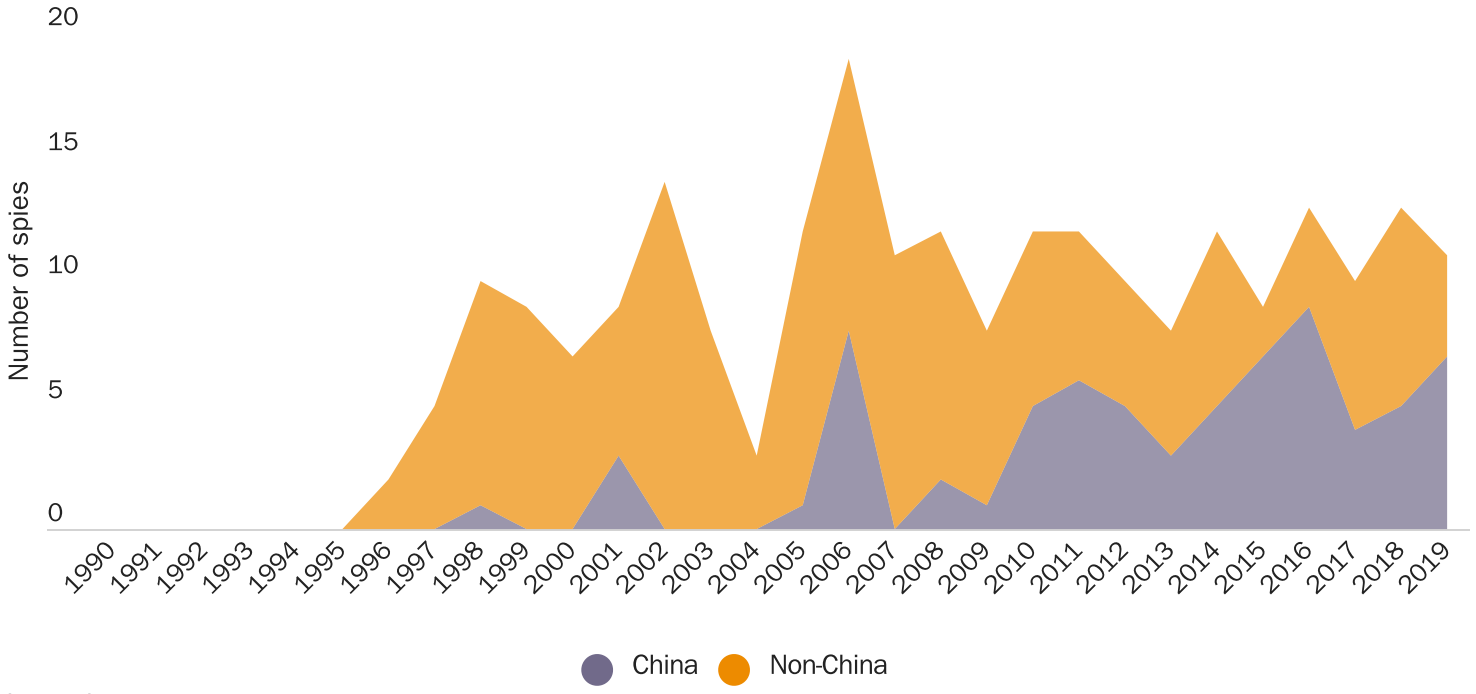
Spies for China by country of birth, 1990–2019

Country of birth	All spies	Percentage of all spies	Spies, AECA excluded	Percentage of spies, AECA excluded
China	171	62.0%	112	64.0%
United States	65	23.6%	42	24.0%
Taiwan	20	7.2%	11	6.3%
India	5	1.8%	2	1.1%
Pakistan	2	0.7%	1	0.6%
Vietnam	2	0.7%	2	1.1%
Fiji	1	0.4%	0	0.0%
Ghana	1	0.4%	1	0.6%
Hong Kong	1	0.4%	1	0.6%
Iran	1	0.4%	0	0.0%
Israel	1	0.4%	0	0.0%
Jordan	1	0.4%	0	0.0%
Malaysia	1	0.4%	1	0.6%
Nigeria	1	0.4%	1	0.6%
North Korea	1	0.4%	0	0.0%
Singapore	1	0.4%	1	0.6%
South Korea	1	0.4%	0	0.0%

Sources: See Methodology section; author's calculations.
Note: AECA = Arms Export Control Act.

Figure 7

Economic espionage, theft of trade secrets, and conspiracy to steal trade secrets, 1990–2019



Source: See Methodology section.

Table 11

Chinese spies prosecuted by the U.S. Department of Justice's China Initiative, 2013–2019

Year	All	China-born	Taiwan-born	Hong Kong–born	U.S. born
2013	1	1	0	0	0
2014	0	0	0	0	0
2015	2	2	0	0	0
2016	0	0	0	0	0
2017	4	2	0	0	2
2018	10	4	4	1	1
2019	13	12	0	0	1

Source: See Methodology section.

> "40 percent of the prosecutions conducted by the Department of Justice's China Initiative are for economic espionage or theft of trade secrets."

who spied for China without setting foot on U.S. soil.[124]

Table 12 shows that 40 percent of the prosecutions conducted by the DOJ's China Initiative are for economic espionage or theft of trade secrets. Another 10 percent are for visa fraud, theft, bribery, failure to disclose conflicts of interest concerning programs receiving federal funds, or filing a false tax return. The other 50 percent are for more traditional espionage or espionage-related crimes, including smuggling, being an unregistered foreign government agent, or gathering or delivering classified defense information.

Of the 30 spies who conducted espionage for China, this analysis was able to identify the original visa for 22 of them. Often, foreign-born people enter the United States on one type of visa and adjust their status to another visa. Their original visa is important because that is where the initial U.S. visa screening process would be most likely to fail, assuming the migrant entered with the intent to spy. Of those for whom data are available, half entered on student visas, four on tourist visas, four were native-born Americans, three entered as lawful permanent residents, and one came as an intracompany transfer.

COST-BENEFIT ANALYSIS

The above analysis shows the scale of state and commercial espionage committed by spies physically present in the United States. Espionage imposes a cost to national security and the economy of the United States, but the existence of costs by themselves does not argue for more government actions to reduce or eliminate them. The costs of government actions to reduce or eliminate espionage must also be accounted for when considering appropriate government responses.

Government risk analyses rarely quantify the costs of espionage and anti-espionage policies. Most are lawyerly documents that are focused on perceived institutional weaknesses and are peppered with anecdotes rather than building a system-wide model of espionage and testing their hypotheses against real-world data. While this type of analysis might be appropriate in some cases, it's an inappropriate guide to setting efficient government policy in the first place, and it does not consider the costs of government actions.

One example of this type of lawyerly risk analysis is the recent Office of the Citizenship and Immigration Services Ombudsman report that attempts to analyze the risk of Chinese students and post-graduate temporary workers in the Optional Practical Training (OPT) program to the United States.[125] It creates a framework to separately examine threat, vulnerability, and consequence to evaluate the risk from those types of Chinese workers. The report claims that its threat and vulnerability analysis

> help us to understand the probability of a danger arising in activities around

Table 12

Chinese spies prosecuted by the U.S. Department of Justice's China Initiative by main crimes, 2013–2019

	Spies
Agent of a foreign government	4
Conspiracy to defraud the United States	1
Conspiracy to steal trade secrets	2
Economic espionage	10
Filing false tax return	1
Gathering or delivering defense information to aid a foreign government	1
International Emergency Economic Powers Act	1
Smuggling	6
Theft, bribery, failure to disclose conflicts of interest concerning programs receiving federal funds	2
Unlawful retention/communication of national defense information	1
Visa fraud	1

Source: See Methodology section.

> the program; consequence analysis helps us to understand the nature and magnitude of the danger. These three together help us to determine whether activity around the program manifests low, medium or high levels of risk. This approach is incremental; if at any point in the analysis there is no perceived threat, or vulnerability, or consequence, then little or no risk is manifested and the analysis can conclude. However, if some level of risk exists within the program, it becomes necessary to examine strategies to mitigate or eliminate the risk.[126]

The ombudsman's threat analysis examines whether Chinese students and OPT workers could harm the United States by analyzing their level of access, their intent, and their capabilities. The access variable is how Chinese people on these visas can leverage their access to the advantage of foreign governments and to the disadvantage of the United States. The intent variable is whether Chinese workers and students intend to engage in actions detrimental to the United States. The capabilities variable is whether those persons have the technical and organizational capabilities to harm the United States and aid foreign governments.[127]

They have access because there are many Chinese students and post-graduate temporary workers who frequently are employed in technical fields that grant them access to commercial and trade secrets or other potentially valuable information. There seems to be intent because Chinese government programs likely incentivize commercial espionage and theft of trade secrets.[128] The ombudsman report's section on capability is the weakest, as it relies on three arguments that are either only partly relevant, supported by little evidence, or both. The first is that the Chinese government is using spies in the United States to help foreign hackers gain access. The primary example is Dejan Karabasevic, a Serbian national who worked for an American firm in Austria and helped a Chinese firm gain access to its secrets.[129] Since Karabasevic was not a Chinese student nor on a temporary work program in the United States, his crime is not relevant to the ombudsman's risk analysis. The second example focuses on the alleged economic espionage of Chinese-born Liu Ruopeng, who was not actually charged with economic espionage because the case was likely weak.[130] Again, a Chinese student not charged with economic espionage is not evidence of Chinese capability to commit economic espionage. The third statement argues that China has the

"Again, a Chinese student not charged with economic espionage is not evidence of Chinese capability to commit economic espionage."

"The simplest way to value state espionage is to look at the price that foreign governments are willing to pay for it."

capability because the DOJ established the China Initiative to counter China's capability, which is circular reasoning.[131]

The ombudsman report next claims that student visas and post-graduate work permits are vulnerable because students and workers are not tracked perfectly while they are in the United States; they can reside here for many years; there is some fraud or noncompliance with the regulations; and there is not enough federal oversight. Of course, few, if any, of these regulations are intended to prevent espionage. If a post-graduate temporary worker is employed on paper at a shell company that doesn't actually conduct research while remaining in the United States, then that person does not have access to sensitive information, so there is no threat. The reasoning applies to a Chinese student enrolled at a fictitious university where the student doesn't have access to any actual secrets. Interestingly, this section relies again on the irrelevant Liu Ruopeng anecdote. The ombudsman report states that it will "help us to understand the probability of a danger arising in activities around the program," but it provides no such probability.[132]

The rest of this section uses the numbers of spies to examine the costs of espionage and the costs of some policies proposed to stop or reduce espionage, as well as whether those government policies pass a simple cost-benefit test. The cost-benefit analysis will consider the policy of a total moratorium on future Chinese immigration and temporary travel to the United States, the cancellation of temporary visas for Chinese students currently studying at American universities, and the exclusion of Chinese workers in the OPT program and on the H-1B visa.

Estimating the Costs of Espionage

When he sentenced China-born spy Dongfan "Greg" Chung for economic espionage and being an unregistered agent of a foreign government in 2010, Judge Cormac J. Carney said that he could not "put a price tag" on national security—but he implicitly did so when he sentenced Chung to a prison term of nearly 16 years.[133] Everything has a price, and the actions of courts, government bureaucrats, and people in their everyday lives reveal that to be true even in the case of human life. The value of a statistical life (VSL) indicates the tradeoff rate between fatality risk and money for a person. Nobody values his life infinitely. All people voluntarily make decisions that increase the chance that they will die, like voluntarily driving an automobile, because they value their life at a certain amount and favorably compare the risk of the activity ending their life with the benefits of the activity. Analyzing public policy actions through the lens of the VSL is common in health economics, labor economics, legal cases, and national security.[134] In the case of national security, the U.S. Department of Homeland Security valued a statistical life at $13 million when considering anti-terrorism policies, and more recent studies place that value at around $10 million for lives not lost by violence.[135]

The VSL is dollar denominated because it's a common unit of exchange and value that has alternative uses, meaning it's easier to gauge tradeoffs and opportunity cost using dollars than by using any other unit. This doesn't mean that money is the only thing that people value, but it reduces those other things we value to a common unit that is more easily comparable. If the price of human life can be estimated, debated, and used in public policy, then surely the price of espionage can also be estimated, contrary to Carney's statement.

The first step is estimating the cost of state espionage per spy. Estimating the cost of Chinese espionage to the United States is more difficult than estimating the VSL. The cost of state espionage to the United States could be the deployment of a new weapons system by China, advances in Chinese research that could affect national security, the relative weakening of the United States, the discovery and arrest of American agents in China, or myriad other factors that are difficult to price. The simplest way to value state espionage is to look at the price that foreign governments are willing to pay for it—an admittedly imperfect but

straightforward method.[136] The most highly paid spy in U.S. history was Aldrich Hazen Ames, who was paid a total of $4.6 million by the Soviets by the time of his arrest in 1994.[137] Adjusted for inflation, Ames was paid just over $8 million for his state espionage. This analysis uses the rounded-up figure of $10 million, the highest recorded pay for a spy engaged in state espionage, plus a premium to guarantee that the cost estimates err on the side of being too high for the cost of each spy engaged in state espionage in the United States.

The next step is estimating the cost of commercial espionage per spy. The estimates of the total cost of economic espionage, theft of trade secrets, and theft of intellectual property (IP) are methodologically muddled and unsound.[138] They essentially estimate the size of other black-market activities, such as narcotics trafficking and tax evasion, compare them to research and development spending, assume those black-market activities are a proxy for the cost of IP theft, and then eyeball the estimates at about 1–3 percent of GDP without any statistical analysis.[139] Implicit in those analyses is that information and secrets are rivalrous. In reality, the costs of these crimes lower monopoly rents for American firms. Worse, the cost estimates do not seriously consider the disincentive to invest in research and development that pervasive economic espionage, theft of trade secrets, and IP theft could impose. That faulty analysis means we must look elsewhere.

Thus, this paper looks at the damages paid in economic espionage court decisions. These damages are determined by several legal theories, such as income models based on unjust enrichment, cost models based on the replacement cost, and market value models based on the fair market value of the economic secret. According to an analysis of economic espionage cases published in the *Duke Law and Technology Review*, the highest award in a single American court case of theft of trade secrets was $250 million excluding attorney's fees and punitive damages, but the average was less than $5 million. This paper thus estimates that each spy who engages in economic espionage or theft of trade secrets costs the United States $250 million.[140] The state-espionage cost estimate of $10 million per spy and the economic espionage cost estimate of $250 million per spy are based on extreme outliers, but they are applied in every instance so that if the cost-benefit analysis errs, it errs in the direction of *overestimating* the costs.

Estimating the Costs of a Moratorium on Chinese Immigration and Travel

The next step is estimating the cost to gross domestic product (GDP) of a moratorium on Chinese travel and immigration, as well as the revocation of student visas, OPT, and H-1B visas for Chinese nationals. The loss from halting the flow of Chinese immigrants is equal to the annual flow in 2018, the last year of data available, multiplied by the average wages spread among all immigrants, including the nonworkers, which is equal to about $2.1 billion.[141] The contribution of Chinese tourists to GDP in 2018 comes from the travel exports for China, subtracting the benefits of education to avoid double counting, which is about $21.2 billion.[142] The contribution of Chinese students is equal to their share of the foreign student population multiplied by their total contribution to GDP in 2018, which is equal to about $15.2 billion.[143] The contribution of Chinese workers on OPT is their number multiplied by the average wage for OPT workers in 2018, which is about $6.1 billion.[144] The contribution of Chinese workers on the H-1B visa is estimated by taking their share of H-1B visa approvals in 2018 multiplied by the estimated stock of H-1B visas. That product is then multiplied by their average wage for approved H-1B workers in 2018, which is about $4.1 billion.[145] The sum of those costs to GDP of a moratorium and revocation of Chinese visas would be about $48.8 billion in the first year.

Calculating the Break-Even Point

The cost imposed by a single spy engaged in state espionage is estimated at $10 million; the cost imposed by a single spy engaged in

"The state-espionage cost estimate of $10 million per spy and the economic espionage cost estimate of $250 million per spy are based on extreme outliers."

> "A moratorium and revocation of Chinese visas does not come close to passing a cost-benefit test even under assumptions very favorable to those who support restrictions."

economic espionage and theft of trade secrets is estimated at $250 million; and the costs of canceling all Chinese tourism and immigration, as well as revoking temporary visas, would be equal to about $48.8 billion in the first year. In 2019, the government identified eight Chinese-born spies who were engaged in state espionage that imposed a cost of $80 million. In 2019, the government identified seven spies who committed economic espionage or theft of trade secrets who imposed a total cost of $1.75 billion on the U.S. economy. A moratorium on Chinese immigration and a revocation of their existing visas would have to annually prevent 4,875 Chinese spies engaged in state espionage, or 195 Chinese spies engaged in economic espionage or theft of trade secrets, to break even.

A moratorium on new Chinese immigration and travel, combined with a revocation of existing visas, would have to annually prevent 609 times as many Chinese spies engaged in state espionage than who were identified at the height of the DOJ's China Initiative. A moratorium on new Chinese immigration and travel, combined with a revocation of existing visas, would have to annually prevent almost 28 times as many Chinese spies engaged in economic espionage or theft of trade secrets than those who were identified at the height of the initiative.

A new immigration policy like this, intended to decrease Chinese espionage, would have to annually prevent more than 80 times as many Chinese spies engaged in state espionage than have been identified over the past 30 years combined to break even. Similarly, this policy would have to prevent about 3.5 times as many Chinese spies engaged in economic espionage and theft of trade secrets every year than have been discovered over the past 30 years combined. It could be that the costs of state espionage are particularly difficult to assess, as the information passed by Ames resulted in the exposure of many American spies in the Soviet Union and the potential relative weakening of U.S. security, so perhaps this analysis oversteps on examining the costs of state espionage.

A moratorium and revocation of Chinese visas does not come close to passing a cost-benefit test even under assumptions very favorable to those who support restrictions. This result holds even if the number of unidentified Chinese spies is many times greater than the number who have been identified.

Chinese Responses to an Immigration Moratorium

Even if a moratorium on travel and immigration from China produced the best possible outcome of reducing the number of Chinese-born spies on U.S. soil to zero, the Chinese government would react in ways to nullify that decline. There are at least two ways in which they would do so. The first is by increasing their efforts to recruit native-born American spies or spies born in other countries. Table 10 shows the number of spies who spied for China by their country of origin: 38 percent were not born in China, including 23.6 percent who were born in the United States. The second is by increasing espionage through sources other than human intelligence on U.S. soil, such as through increasing resources devoted to computer hacking from China. Espionage is a dynamic and adaptive sector, so the Chinese government's reaction to an immigration and travel moratorium could recover some espionage capability while the United States absorbs a large and annually increasing cost by blocking travel and immigration from China. In such a scenario, the benefits described above could be even smaller.

GOVERNMENT ACTIONS TO REDUCE CHINESE ESPIONAGE AND ESPIONAGE-RELATED CRIMES

A moratorium on Chinese immigration and travel, and a revocation of visas for Chinese nonimmigration, would do much more damage to the United States than even the most extreme estimates of the costs of espionage. Those costs don't include other potential costs, such as locking out brilliant Chinese

scientists who would have contributed to science, technology, and the U.S. economy. Instead, those scientists would contribute to Chinese research, where they could benefit the Chinese government.

One example of this is research to create artificial intelligence (AI), which could have profound effects on humanity and national security. Of notable Chinese-trained AI specialists, 63 percent have immigrated to the United States, and only 26 percent have remained in China since 2010.[146] Blocking immigration from China may prevent a few spies from entering the United States, but it would also drastically reduce the supply of Chinese AI researchers for America and increase the supply in China. Of the international AI researchers who eventually worked for U.S.-based companies and institutions, 27 percent came from China, and only 31 percent were native-born Americans. Unless the goal is to hurt U.S.-led efforts to develop AI and subsidize China, blocking immigration from China would be a big mistake.[147]

The U.S. government has made that mistake before, during the Cold War.[148] Qian Xuesen immigrated from China and earned his PhD from Cal Tech in 1939. He was a pioneer in cybernetics, aerospace engineering, and physics. He was involved with the Manhattan Project and designing American rockets. Theodore von Kármán, a legendary aerospace engineer, mathematician, and physicist, pronounced Xuesen an "undisputed genius." During the Cold War, Xuesen was accused of being a communist on flimsy evidence. He lost his security clearances, and his career options were limited. He decided to return to China and was detained by U.S. authorities for five years under house arrest after the government claimed that he was trying to smuggle out classified documents. Subsequent examination of the documents that he possessed showed they contained no classified material. Eventually, Xuesen was traded to China in exchange for downed American pilots. In China, Xuesen helped lead the Chinese nuclear weapons and missile programs, earning the moniker "Father of Chinese Rocketry." Undersecretary of the U.S. Navy Dan A. Kimball, who knew Xuesen personally, said, "It was the stupidest thing this country ever did. He was no more a Communist than I was, and we forced him to go."[149] How many brilliant Chinese scientists like Xuesen has the U.S. government already turned away or will turn away if it adopts a restrictive anti-Chinese immigration policy?

There are many policy options available to Congress and the president to reduce Chinese espionage without aiding the Chinese government or hurting the U.S. economy or national security. It is vital that policy be based on available evidence rather than giving in to the temptation to inflate threats. Current immigration law appropriately designates aliens as inadmissible if they are suspected or known spies, which includes commercial and state espionage and suspected or known violators of U.S. export-control laws such as the AECA.[150] Immigration law also designates Communist Party members and their immediate families as inadmissible with certain exceptions, such as if they were involuntarily members of the Communist Party or if they joined merely to get a job.[151] The Chinese Communist Party has approximately 92 million members and at least as many immediate family members; most of them likely joined to help their careers in that totalitarian state. It's very difficult for the U.S. government to enforce this rule because it can't identify who is a Communist Party member, so it's likely a dead letter even though the Trump administration considered enforcing a total immigration ban on them.[152] However, targeted bans against known Communist Party members in positions of authority can be enforced and might be appropriate, although the Chinese government would likely adapt to this by making party membership even more secretive, so the effectiveness of such a ban on reducing espionage would likely be negligible to nonexistent.

The portion of the DOJ's China Initiative that informs universities about the terms of their government grants and lets U.S. firms know about criminal investigations that affect

"Unless the goal is to hurt U.S.-led efforts to develop artificial intelligence and subsidize China, blocking immigration from China would be a big mistake."

"Over time, the rate of Chinese students returning to China has increased."

firms in the same economic sector or region of the country is completely appropriate and should be stepped up.[153] American firms are the biggest victims of economic espionage and theft of trade secrets, but they are also big beneficiaries of hiring foreign-born talent. The DOJ's efforts to inform them about espionage investigations will allow U.S. firms to balance risks more accurately to price in their hiring decisions and expenditures on internal security, enabling them to efficiently reduce this type of espionage. If, after knowing the risks, these firms still hire workers who are more likely to be commercial spies and they are the victims of commercial espionage, then they bear most of the costs, as they should. In this way, if the government increases enforcement efforts, then firms would likely underinvest in security and free ride on the government-provided security, which would result in more commercial espionage.

The National Institutes of Health (NIH) is probing whether grantees have disclosed their foreign ties and has found many scientists with undisclosed links to China, but the vast majority are likely innocuous, are the result of bureaucratic oversights, and have no connection to espionage.[154] Espionage isn't even the main justification for enforcing the NIH grant guidelines. The agency doesn't mention espionage as a reason for its probe in discussions with universities about the problem of undeclared foreign ties. Instead, the NIH focuses on how undeclared foreign ties can steal a researcher's time from other projects and create redundancy between NIH grants that wastes government funds, as well as showing that such foreign ties distort the NIH's accounting of the amount of funding for specific research agendas. It's important for the NIH to balance enforcing the law with not scaring away foreign-born grantees or their American-born coresearchers, as well as not exaggerating the potential espionage issues.[155]

The government could go further to expose Chinese espionage. The Chinese Thousand Talent Program offers a starting bonus of about $150,000 for a talented Chinese-born researcher to return to China, as well as large research grants.[156] Even with these large incentives, they have only had limited success in attracting talent from abroad who could potentially be commercial spies.[157] Over time, the rate of Chinese students returning to China has increased, in part because of the government incentives and also because of the increasing relative economic opportunity in China.[158] This rate of return could be cut if the U.S. government offered an easier path to permanent residency for Chinese students, skilled workers, and Chinese researchers in China. Immigration backlogs frustrated many skilled immigrants, so removing these backlogs, especially for skilled Chinese immigrants, will incentivize some of them to stay in the United States or immigrate in the first place.[159] The government could also use the national-interest waiver provision of U.S. law, combined with increasing the total number of employment-based green cards, to allow Chinese researchers to stay here more easily.[160] In other words, lowering the cost for skilled Chinese immigrants to remain in the United States could counter the Chinese government's funding schemes.

The U.S. government could also incentivize foreign-born spies to come forward with a promise of amnesty and a green card so long as they provide evidence that they were spies, what they spied on, and how they did it; and/or if they identify other spies, weaknesses in U.S. security, and their contacts in China. Importantly, such an incentive would have to be only retroactively applied to discourage non-spies from starting to spy just so they can get a green card. The U.S. government could also offer cash rewards if the spying occurred prior to the date at which the award was announced, so as not to encourage spying, with a clear statement that this is a one-time offer. Such a policy would be especially attractive now because the DOJ's China Initiative is increasing the likelihood that spies will be caught, and an amnesty with a green card would provide a way out instead of deportation or jail. At a minimum, such a policy would mean that those spies won't

return to China and would teach the American government more about Chinese espionage operations in the United States. There are downsides to this from a counterintelligence perspective—it may add more confusion than clarity regarding Chinese intelligence—but that could be limited by targeting the amnesty toward economic spies exclusively.

Lastly, the government should focus more on obstructing hacking from Chinese intelligence agencies in China and reducing the value of American targets for hacking. In 2014, Chinese hackers broke into the Office of Personnel Management and stole records on roughly four million current and past federal employees. According to government emails sent to the victims of the hacking, the stolen records contained the "name, Social Security number, address, date and place of birth, residency, educational, and employment history, personal foreign travel history, information about immediate family as well as business and personal acquaintances, and other information used to conduct and adjudicate your background investigation."[161]

Information to conduct and adjudicate background investigations for security clearances could be especially damaging because that includes personal financial information and details on marital infidelity that could be used by Chinese intelligence agencies to blackmail American government employees. Going forward, the government should take efforts to reduce the possibility of this reoccurring by reducing the scope of federal government employee information retained in government databases as well as better protecting the information retained in the databases. In short, the federal government should update its security and remove much of the temptation to hack it in the first place.

CONCLUSION

This policy analysis presents the first database of identified commercial and state spies who operated on U.S. soil from 1990 through 2019. This form of espionage is a low-probability event. During that time, 1,485 spies engaged in commercial and state espionage were identified on U.S. soil. Of those, 890 were foreign-born, 583 were native-born Americans, and 12 had unknown origins. Native-born Americans accounted for 39.3 percent of all spies, foreign-born spies accounted for 59.9 percent, and spies from unknown origins accounted for 0.8 percent.

The federal government has an important role in limiting espionage, and many people are justifiably worried about efforts by China to spy on the United States. However, ending visas for Chinese nationals would impose a far greater cost on the United States than any potential benefit from reducing espionage. This quantitative analysis of espionage in the United States can hopefully aid the U.S. government in constructing a robust anti-espionage response that does more good than harm.

"The federal government has an important role in limiting espionage."

NOTES

1. "Espionage Law and Legal Definition," USlegal.com.

2. Charles Doyle, "Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act," Congressional Research Service, August 19, 2016; and "Espionage Law and Legal Definition."

3. Sun Tzu, *The Art of War*, trans. Thomas Cleary (New York: Shambhala Publications, 2005), p. 163.

4. Jerrold L. Schecter and Peter S. Deriabin, *The Spy Who Saved the World: How a Soviet Colonel Changed the Course of the Cold War* (New York: Brassey's Inc., 1995).

5. Michael P. Colaresi, *Democracy Declassified: The Secrecy Dilemma in National Security* (New York: Oxford University Press, 2014), pp. 5, 51–53.

6. Gus Weiss, "The Farewell Dossier," Central Intelligence Agency, April 14, 2007; and *Soviet Acquisition of Western Technology* (Washington: Central Intelligence Agency, April 1982).

7. Michael Dougherty, *Annual Report 2020: Citizenship and Immigration Services Ombudsman* (Washington: U.S. Department of Homeland Security, June 30, 2020), p. 76.

8. Steven Novella, "Scientific Fraud in China," Science-Based Medicine, November 27, 2019; and Stuart Ritchie, *Science Fictions: How Fraud, Bias, Negligence, and Hype Undermine the Search for Truth* (New York: Metropolitan Books, 2020), p. 70.

9. Ritchie, *Science Fictions*, p. 70; and Qing-Jiao Liao et al., "Perceptions of Chinese Biomedical Researchers towards Academic Misconduct: A Comparison between 2015 and 2010," *Science and Engineering Ethics* 24, no. 2 (April 10, 2017), https://doi.org/10.1007/s11948-017-9913-3.

10. Ritchie, *Science Fictions*, p. 159; and Taixiang Wu et al., "Randomized Trials Published in Some Chinese Journals: How Many Are Randomized?," *Trials* 10, no. 46 (July 2, 2009), https://doi.org/10.1186/1745-6215-10-46.

11. Weiss, "Farewell Dossier."

12. Albrecht Glitz and Erik Meyersson, "Industrial Espionage and Productivity," *American Economic Review* 110, no. 4 (April 1, 2020): 1055–103, https://doi.org/10.1257/aer.20171732.

13. Glitz, "Industrial Espionage," 1055.

14. Catherine Matacic, "Cold War Espionage Paid Off—Until It Backfired, East German Spy Records Reveal," *Science*, American Association for the Advancement of Science, July 31, 2017.

15. Matacic, "Cold War Espionage"; and Kristie Macrakis, "Does Effective Espionage Lead to Success in Science and Technology? Lessons from the East German Ministry for State Security," *Intelligence and National Security* 19, no. 1 (March 2004), https://doi.org/10.1080/0268452042000222920.

16. U.S. Department of Justice, "Attorney General Jeff Session's (sic) China Initiative Fact Sheet," November 1, 2018.

17. "Information about the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions since 2018," U.S. Department of Justice, updated November 12, 2020.

18. U.S. Department of Justice, "Transcript of Attorney General Barr's Remarks on China Policy at the Gerald R. Ford Presidential Museum," July 17, 2020.

19. Alex Hontos et al., "Insight: Research Institutions under DOJ's False Claims Microscope after Chinese Influence Settlement," *Bloomberg Law*, February 12, 2020; Office of Public Affairs, "Two Former Executives of the China Subsidiary of a Multi-Level Marketing Company Charged for Scheme to Pay Foreign Bribes and Circumvent Internal Accounting Controls," U.S. Department of Justice, November 14, 2019; Office of Public Affairs, "Four Chinese Nationals and Chinese Company Indicted for Conspiracy to Defraud the United States and Evade Sanctions," U.S. Department of Justice, July 23, 2019; Office of Public Affairs, "Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting over 78 Million People," U.S. Department of Justice, May 9, 2019; Office of Public Affairs, "Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets," U.S. Department of Justice, April 23, 2019; Office of Public Affairs, "Chinese National Sentenced to Prison for Selling Counterfeit Computer Parts," U.S. Department of Justice, February 15, 2019; Office of Public Affairs, "Chinese Telecommunications Device Manufacturer and Its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice," U.S. Department of Justice, January 28, 2019; Office of Public Affairs, "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting

Intellectual Property and Confidential Business Information," U.S. Department of Justice, December 20, 2018; Office of Public Affairs, "Former Head of Organization Backed by Chinese Energy Conglomerate Convicted of International Bribery, Money Laundering Offenses," U.S. Department of Justice, December 5, 2018; Office of Public Affairs, "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," U.S. Department of Justice, October 30, 2018; and Office of Public Affairs, "Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies," U.S. Department of Justice, October 10, 2018.

20. "China Initiative Conference," Center for Strategic and International Studies, February 6, 2020, video; Alex Joske, *Hunting the Phoenix: The Chinese Communist Party's Global Search for Technology and Talent* (Canberra, Australia: Australian Strategic Policy Institute), Policy Brief Report no. 35/2020, August 2020; and "Information about the Department of Justice's China Initiative," U.S. Department of Justice.

21. Alexandra Yoon-Hendricks, "Visa Restrictions for Chinese Students Alarm Academia," *New York Times*, July 25, 2018.

22. "US Revokes Visas for 1,000 Chinese Students Deemed Security Risk," *BBC News*, September 10, 2020.

23. Jeffrey Mervis, "Fifty-Four Scientists Have Lost Their Jobs as a Result of NIH Probe into Foreign Ties," *Science*, American Association for the Advancement of Science, June 12, 2020.

24. Tulsi Kamath, "US Orders China to Close Houston Consulate amid Swirling Accusations of Espionage, Theft," Click2Houston.com, July 21, 2020; and Emily Feng, "U.S. Orders China's Houston Consulate to Close, Ratcheting Tensions," NPR, July 22, 2020.

25. Office of the Spokesperson, "'Confucius Institute U.S. Center' Designation as a Foreign Mission," U.S. Department of State, August 13, 2020.

26. James Andrew Lewis, "How Scary Is TikTok?," Center for Strategic and International Studies, July 14, 2020; Billy Easley II, "Banning TikTok and Tencent Isn't a National Strategy against China," *Medium*, August 17, 2020; Julian Sanchez, "A Self-Destructive War on Chinese Software," *Cato at Liberty* (blog), Cato Institute, August 13, 2020; and Brian Fung, "US Will Ban WeChat and TikTok Downloads on Sunday," *CNN Business*, September 18, 2020.

27. John H. Cochrane, "TikTok Dust Up," *Grumpy Economist* (blog), August 13, 2020; and Ryan McMorrow, "Former Chinese Government Official Ran TikTok's Content Policy as App Went Global," *Financial Times*, October 3, 2020.

28. Colaresi, *Democracy Declassified*, p. 115.

29. James Fontanella-Khan and Miles Kruppa, "TikTok Set to Become a Standalone US Company to Satisfy White House," *Financial Times*, September 15, 2020; and Martin Baccardax, "Microsoft, Walmart Shares Gain amid TikTok Sale Deadline Questions," *TheStreet*, September 10, 2020.

30. Fung, "US Will Ban WeChat and TikTok"; Ana Swanson and David McCabe, "U.S. Judge Temporarily Halts Trump's WeChat Ban," *New York Times*, September 20, 2020; Jeanne Whalen, "Federal Court Issues Preliminary Injunction Halting Administration's Ban of Chinese App WeChat," *Washington Post*, September 21, 2020; and Brian Fung and Sherisse Pham, "TikTok Granted Two More Weeks to Reach a Deal for US Business," CNN, November 13, 2020.

31. Dougherty, *Annual Report 2020*.

32. Gerald F. Seib, "How Trump Has Changed the Republicans," *Wall Street Journal*, August 21, 2020.

33. Protecting America from Spies Act, H.R. 7326, 116th Cong. (2020).

34. Office of Senator Tom Cotton, "Cotton, Blackburn, Kustoff Unveil Bill to Restrict Chinese STEM Graduate Student Visas & Thousand Talents Participants," May 27, 2020.

35. Editorial Board, "Trump, TikTok and Crony Capitalism," *Wall Street Journal*, September 20, 2020.

36. U.S.-China Economic and Security Review Commission, *2016 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington: U.S.-China Economic and Security Review Commission, November 2016), pp. 289–92.

37. Alastair Iain Johnston et al., *The Cox Committee Report: An Assessment* (Washington: Carnegie Endowment for International Peace, December 1999).

38. Peter Mattis, "A Guide to Chinese Intelligence Operations," *War on the Rocks*, August 18, 2015.

39. Mattis, "Guide to Chinese Intelligence Operations."

40. Dougherty, *Annual Report 2020*, p. 76.

41. U.S. Senate Permanent Subcommittee on Investigations, "Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans," U.S. Senate Committee on Homeland Security and Governmental Affairs, November 18, 2019; Ritchie, *Science Fictions*, p. 177; Katherine Koleski and Nargiza Salidjanova, "China's Technonationalism Toolbox: A Primer," U.S.-China Economic and Security Review Commission issue brief, March 28, 2018; *Hearing on China's Non-traditional Espionage against the United States before the Committee on the Judiciary U.S. Senate*, 115th Cong. (December 12, 2018) (statement of John C. Demers, Assistant Attorney General); and Damien Ma, "Losing Face: Why China Can't Stop Squandering Its Soft Power," *The Atlantic*, May 14, 2012.

42. U.S. Senate Permanent Subcommittee on Investigations, "Threats to the U.S. Research Enterprise," p. 2.

43. U.S. Senate Permanent Subcommittee on Investigations, "Threats to the U.S. Research Enterprise," pp. 2–3; and David Zweig and Siqin Kang, "America Challenges China's National Talent Programs," Center for Strategic and International Studies, May 2020.

44. Ritchie, *Science Fictions*, pp. 177–78, 182; and Smriti Mallapaty, "China Bans Cash Rewards for Publishing Papers," *Nature* 579, no. 7797 (February 28, 2020), https://doi.org/10.1038/d41586-020-00574-8.

45. Ritchie, *Science Fictions*, p. 182; and Wei Quan, Bikun Checn, and Fei Shu, "Publish or Impoverish: An Investigation of the Monetary Reward System of Science in China," *Aslib Journal of Information Management* 69, no. 5 (September 18, 2017).

46. "China Initiative Conference," Center for Strategic and International Studies, February 6, 2020, video; and "Online Event: Countering Chinese Espionage," Center for Strategic and International Studies, August 12, 2020, video.

47. Colaresi, *Democracy Declassified*, pp. 115–17.

48. "Sample Cases," MSR Visual Compliance, December 13, 2002, http://web.mit.edu/1.265/www/Export%20Penalty%20Cases.pdf; and Joske, *Hunting the Phoenix*, p. 22.

49. See case of Elliot Doxer caught in a U.S. Federal Bureau of Investigation sting in which agents pretended to be from Israel. Counterintelligence Directorate, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (Washington: Defense Security Service, February 2013), p. 6.

50. 18 U.S.C. § 371 (2018).

51. 18 U.S.C. § 793 (2018); and 18 U.S.C. § 1924 (2018).

52. 18 U.S.C. § 794 (2018).

53. 18 U.S.C. § 795 (2018).

54. 18 U.S.C. § 951 (2018).

55. 18 U.S.C. § 2332 (2018).

56. Atomic Energy Act of 1954, 42 U.S.C. § 2011 (2018); and 42 U.S.C. ch. 23.

57. Intelligence Identities Protection Act of 1982, Pub. L. 97–200, 50 U.S.C. §§ 421–426 (2011); and 50 U.S.C. § 3121 (2018).

58. 18 U.S.C. § 666 (2018).

59. 18 U.S.C. § 1032 (2018).

60. 18 U.S.C. § 641 (2018).

61. 18 U.S.C. § 842 (2018).

62. Arms Export Control Act of 1976, 22 U.S.C. §§ 2751–2799 (2018); and "Debarred Parties," Directorate of Defense Trade Controls, U.S. Department of State, https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=c22d1833dbb8d300d0a370131f9619f0.

63. Intelligence Identities Protection Act of 1982, Pub. L. 97–200, 50 U.S.C. §§ 421–426 (2011); and 50 U.S.C. §§ 1701–1706 (2011).

64. 18 U.S.C. § 1831 (2018).

65. 18 U.S.C. § 1832 (2018).

66. 18 U.S.C. § 287 (2018).

67. 18 U.S.C. § 1832 (2018).

68. 18 U.S.C. § 1001 (2018).

69. 18 U.S.C. § 1343 (2018).

70. 18 U.S.C. § 1503 (2018).

71. 18 U.S.C. § 1519 (2018).

72. 18 U.S.C. § 1546 (2018).

73. 18 U.S.C. § 554 (2018).

74. 18 U.S.C. § 201 (2018).

75. 26 U.S.C. § 7206 (2018).

76. Arms Export Control Act of 1976, 22 U.S.C. § 2778 (2018).

77. Federal Bureau of Investigation, Los Angeles Division, "Ex-Marine Accused of Attempting to Export Sensitive Military Items," press release, March 5, 2012.

78. 8 U.S.C. § 1182(a)(3)(A)(i) (2011).

79. U.S. Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases," January 2018, pp. 28–29.

80. Office of Public Affairs, "Retired University Professor Sentenced to Four Years in Prison for Arms Export Violations Involving Citizen of China," U.S. Department of Justice, July 1, 2009.

81. U.S. Department of Justice, "Summary of Major U.S. Export Enforcement," p. 37.

82. "Debarred Parties," Directorate of Defense Trade Controls.

83. "Sample Cases," MSR Visual Compliance, p. 23.

84. "Cartel Suspects Arrested in Miami Arms-Buying Plot," *Deseret News*, May 7, 1990.

85. Richards J. Heuer Jr. and Katherine Herbig, "Espionage by the Numbers: A Statistical Overview," U.S. Department of Commerce, Office of Security, Western Region Security Office, November 28, 2001.

86. Alex Nowrasteh, "Terrorists by Immigration Status and Nationality: A Risk Analysis, 1975–2017," Cato Institute Policy Analysis no. 866, May 7, 2019; and Alex Nowrasteh, "Terrorism and Immigration: A Risk Analysis," Cato Policy Analysis no. 798, September 13, 2016.

87. "Information about the Department of Justice's China Initiative," U.S. Department of Justice.

88. U.S. Department of Justice, "Jeff Session's China Initiative Fact Sheet"; and "China Initiative Conference," Center for Strategic and International Studies.

89. "FBI Launches Criminal Investigation into NSA Leaks," *VOA News*, June 14, 2013; and Trevor Aaronson, "A Declassified Court Ruling Shows How the FBI Abused NSA Mass Surveillance Data," *The Intercept*, October 10, 2019.

90. Nicole Perlroth, "Accused of Spying for China, until She Wasn't," *New York Times*, May 9, 2015; and William W. Fick, Daniel N. Marx, and Amy Barsky to the U.S. District Court for the District of Massachusetts, "Memorandum in Support of Motion to Dismiss Indictment due to Unconstitutional Selective Enforcement and Prosecution," *United States v. Haoyang Yu et al.*, no. 19-cr-10195-WGY, June 22, 2020.

91. Shawn L. Twing, "Pentagon, GAO Report Israeli Espionage and Illegal Technology Retransfer," *Washington Report on Middle East Affairs*, April 1996.

92. Zachary Keck, "Robert Gates: Most Countries Conduct Economic Espionage," *The Diplomat*, May 23, 2014.

93. Kim Zetter, "Code Not Physical Property, Court Rules in Goldman Sachs Espionage Case," *Wired*, April 11, 2012.

94. David E. Pozen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information," *Harvard Law Review* 127, no. 512 (December 20, 2013).

95. Cynthia McFadden, Aliza Nadi, and Courtney McGee, "Education or Espionage? A Chinese Student Takes His Homework Home to China," *NBC News*, July 24, 2018.

96. Katherine L. Herbig, *The Expanding Spectrum of Espionage by Americans, 1947–2015* (Seaside, CA: Defense Personnel and Security Research Center, August 2017).

97. Jeremy S. Wu, "Federal Cases," Jeremy S. Wu, https://

jeremy-wu.info/fed-cases/.

98. "Jeremy Wu," Board of Directors, committee100.org.

99. Marjorie A. Meyers and H. Michael Sokolow to Judge Patti B. Saris, "Re: Public Comment on Proposed Amendments for 2013," U.S. Sentencing Commission, Washington, DC, March 19, 2013.

100. Thomas J. Nolan, "Trends in Trade Secret Prosecutions," Noble Barton Bradford & Olmos LLP, 2016.

101. Andrew Chongseh Kim, "Prosecuting Chinese 'Spies': An Empirical Analysis of the Economic Espionage Act," *Cardozo Law Review* 40, no. 2 (December 2018).

102. Joske, *Hunting the Phoenix*.

103. "Debarred Parties," Directorate of Defense Trade Controls.

104. See, for example, Bureau of Industry and Security, U.S. Department of Commerce, "In the Matter of: Viacheslav Zhukov, Register Number: 18963-021, D. Ray James Correctional Institution, P.O. Box 2000, Folkston, GA 31537," 81 Fed. Reg. 8478 (February 19, 2016).

105. Bureau of Industry and Security, *Annual Report to Congress for Fiscal Year 2014* (Washington: U.S. Department of Commerce, December 12, 2014), https://www.bis.doc.gov/index.php/documents/policy-guidance/1183-bis-annual-report-2014/file; and "Export Violations," Bureau of Industry and Security, U.S. Department of Commerce.

106. U.S. Department of Justice, "Summary of Major U.S. Export Enforcement"; "Fact Sheet: Major U.S. Export Enforcement Prosecutions during the Past Two Years," U.S. Department of Justice, October 28, 2008; "Justice News Archive," U.S. Department of Justice (website), https://www.justice.gov/archives/justice-news-archive; U.S. Department of Justice, "Summary of Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases," June 27, 2016; and "Justice News," U.S. Department of Justice.

107. "News Releases," U.S. Immigration and Customs Enforcement.

108. "Bureau of Diplomatic Security: Press Releases," U.S. Department of State Archive, https://2001-2009.state.gov/m/ds/rls/c9360.htm; "News from the Bureau of Diplomatic Security," U.S. Department of State Archive, https://2001-2009.state.gov/m/ds/rls/index.htm; and "DSS Releases," U.S. Department of State, https://www.state.gov/subjects/dss-releases/page/13/?results=30&currpage=2&totalpages=13&coll_filter_year&coll_filter_month&coll_filter_speaker&coll_filter_country&coll_filter_release_type&coll_filter_bureau&coll_filter_program&coll_filter_profession.

109. Please email Alex Nowrasteh at anowrasteh@cato.org for information related to specific individuals.

110. U.S. Census Bureau, IPUMS. *5% Sample*, 1990, 2000; American Community Survey. 1-Year Estimates, 2000–2018; Department of Homeland Security. Nonimmigrant Admissions (I-94 Only) by Region and Country of Citizenship, 1996-2018; Immigration and Naturalization Service. Statistical Yearbook, 1990–1995, https://usa.ipums.org/usa/.

111. Figure 2 only considers the resident and nonimmigration population for the countries that sent at least one spy who was identified during the 1990–2019 period. Those countries, including the United States, account for 98 percent of all residents and a similar percentage of nonimmigrants. Including all U.S. residents and nonimmigrant admissions from countries that did not send a single spy does not affect the results.

112. Steven Aftergood, "The Case of Matthew Diaz," *Secrecy News* (blog), Federation of American Scientists, April 7, 2008.

113. "Online Event: Countering Chinese Espionage," Center for Strategic and International Studies.

114. Carlos Echeverria-Estrada and Jeanne Batalova, "Chinese Immigrants in the United States," Migration Policy Institute, January 15, 2020.

115. U.S. Department of Justice, "Jeff Session's China Initiative Fact Sheet."

116. "Information about the Department of Justice's China Initiative," U.S. Department of Justice.

117. "Information about the Department of Justice's China Initiative."

118. Office of Public Affairs, "Former West Virginia University Professor Pleads Guilty to Fraud That Enabled Him to Participate in the People's Republic of China's 'Thousand Talents

Plan,'" U.S. Department of Justice, March 10, 2020.

119. Office of Public Affairs, "Former Defense Intelligence Officer Arrested for Attempted Espionage," U.S. Department of Justice, June 4, 2018.

120. Office of Public Affairs, "Jury Convicts Former CIA Officer of Espionage," U.S. Department of Justice, June 8, 2018.

121. Office of Public Affairs, "Former State Department Employee Sentenced for Conspiring with Chinese Agents: Received Tens of Thousands of Dollars in Benefits from Two Chinese Agents in Exchange for Internal State Department Documents," U.S. Department of Justice, July 9, 2019.

122. Office of Public Affairs, "Jury Convicts Former CIA Officer of Espionage," U.S. Department of Justice, June 8, 2018; and Office of Public Affairs, "Former Defense Intelligence Officer Arrested for Attempted Espionage."

123. Office of Public Affairs, "Former State Department Employee Sentenced for Conspiring with Chinese Agents."

124. Hontos et al., "Insight: Research Institutions under DOJ's False Claims Microscope"; Office of Public Affairs, "Two Former Executives of the China Subsidiary of a Multi-Level Marketing Company Charged for Scheme"; Office of Public Affairs, "Four Chinese Nationals and Chinese Company Indicted"; Office of Public Affairs, "Member of Sophisticated China-Based Hacking Group Indicted"; Office of Public Affairs, "Former GE Engineer and Chinese Businessman Charged"; Office of Public Affairs, "Chinese National Sentenced to Prison"; Office of Public Affairs, "Chinese Telecommunications Device Manufacturer and Its U.S. Affiliate Indicted"; Office of Public Affairs, "Two Chinese Hackers Associated with the Ministry of State Security Charged"; Office of Public Affairs, "Former Head of Organization Backed by Chinese Energy Conglomerate Convicted"; Office of Public Affairs, "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal"; and Office of Public Affairs, "Chinese Intelligence Officer Charged."

125. Dougherty, *Annual Report 2020*.

126. Dougherty, *Annual Report 2020*, p. 73.

127. Dougherty, *Annual Report 2020*, pp. 73–74.

128. Dougherty, *Annual Report 2020*, pp. 74, 77–79.

129. "Statement of Michael A. Brown, Presidential Innovation Fellow, before the House Permanent Select Committee on Intelligence," U.S. Capitol Visitor Center, July 19, 2018; and Erin Ailworth and Eugen Freund, "Engineer Guilty in Software Theft," Boston.com, September 24, 2011.

130. McFadden, Nadi, and McGee, "Education or Espionage?"

131. Dougherty, *Annual Report 2020*, p. 80.

132. Dougherty, *Annual Report 2020*.

133. U.S. Attorney's Office for the Central District of California, "Former Boeing Engineer Sentenced to Nearly 16 Years in Prison for Stealing Aerospace Secrets for China," press release, FBI, February 8, 2010.

134. Thomas J. Kniesner and W. Kip Viscusi, "The Value of a Statistical Life," *Oxford Research Encyclopedia of Economics and Finance*, forthcoming, Vanderbilt Law School Legal Studies Research Paper Series no. 19-15, April 10, 2019; and John Mueller and Mark G. Stewart, "Responsible Counterterrorism Policy," Cato Institute Policy Analysis no. 755, September 10, 2014.

135. Robert W. Hahn, Randall W. Lutter, and W. Kip Viscusi, *Do Federal Regulations Reduce Mortality?* (Washington: American Enterprise Institute–Brookings Joint Center for Regulatory Studies, 2000); and Benjamin H. Friedman, "Managing Fear: The Politics of Homeland Security," *Political Science Quarterly* 126, no. 1 (2011): 85n31.

136. Espionage may be a monopsonistic market, so the price might be lower because of the purchasing country's market power.

137. "Double Agent CIA KGB Spy: Aldrich Ames, the Highest Paid and Most Dangerous Spy in American History," *Soldier of Fortune*, November 28, 2020.

138. Daniel Takash, "Bad Math on Chinese IP Theft Is Used to Justify Trade War," capturedeconomy.com, Niskanen Center, October 15, 2019; and Commission on the Theft of American Intellectual Property, *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (Washington: National Bureau of Asian Research, 2017).

139. Takash, "Bad Math."

140. Gavin C. Reid, Nicola Searle, and Saurabh Vishnubhakat, "What's It Worth to Keep a Secret?," *Duke Law & Technology Review* 13, no. 1 (2015): 116, 137–40, 149–50.

141. U.S. Department of Homeland Security, *2018 Yearbook of Immigration Statistics* (Washington: U.S. Department of Homeland Security, January 6, 2020), pp. 10–11, table 2; and U.S. Bureau of the Census, *Current Population Survey: 2019 Annual Social and Economic Supplement* (Washington: U.S. Bureau of the Census, 2019).

142. National Travel and Tourism Office, *Fast Facts: United States Travel and Tourism Industry 2018* (Washington: International Trade Administration, October 2019).

143. Erin Duffin, "Number of International Students in the U.S., by Country of Origin 2019/20," Statista.com, November 23, 2020; "Number of International Students in the United States Hits All-Time High," press release, Institute of International Education, November 18, 2019; and "Research Special Reports and Analyses," opendoorsdata.org, Institute of International Education.

144. David J. Bier, "The Facts about Optional Practical Training (OPT) for Foreign Students," *Cato at Liberty* (blog), Cato Institute, May 20, 2020.

145. Office of Policy and Strategy, Policy Research Division, *H-1B Authorized-to-Work Population Estimate* (Washington: U.S. Citizenship and Immigration Services, 2020); and U.S. Citizenship and Immigration Services, *Characteristics of H-1B Specialty Occupation Workers: Fiscal Year 2018 Annual Report to Congress* (Washington: U.S. Department of Homeland Security, April 4, 2019).

146. Joy Dantong Ma, "China's AI Talent Base Is Growing, and Then Leaving," Macro Polo, July 30, 2019.

147. Ishan Banerjee and Matt Sheehan, "America's Got AI Talent: US' Big Lead in AI Research Is Built on Importing Researchers," Macro Polo, June 9, 2020.

148. Alex Nowrasteh, "The Downside of an Ideological Litmus Test for Immigrants," Cato Institute, August 24, 2016.

149. Alex Nowrasteh, "We Should 'Confront' China by Liberalizing Chinese Immigration," *Cato at Liberty* (blog), Cato Institute, May 29, 2020.

150. 8 U.S.C. § 1182(a)(3)(A)(i) (2011).

151. 8 U.S.C. § 1182(a)(3)(D)(i) (2011); and 8 U.S.C. § 1182(a)(3)(D)(ii) (2011).

152. Paul Mozur and Edward Wong, "U.S. Weighs Sweeping Travel Ban on Chinese Communist Party Members," *New York Times*, July 15, 2020.

153. "Online Event: Countering Chinese Espionage," Center for Strategic and International Studies.

154. Jeffrey Mervis, "Fifty-Four Scientists Have Lost Their Jobs"; and Michael S. Lauer, "ACD Working Group on Foreign Influences on Research Integrity Update," (PowerPoint presentation, virtual meeting, National Institutes of Health, June 12, 2020).

155. Jeffrey Mervis, "NIH Letters Asking about Undisclosed Foreign Ties Rattle U.S. Universities," *Science*, American Association for the Advancement of Science, March 1, 2019; and Mervis, "Fifty-Four Scientists Have Lost Their Jobs."

156. Hepeng Jia, "China's Plan to Recruit Talented Researchers," *Nature* 553, S8 (January 17, 2018), https://doi.org/10.1038/d41586-018-00538-z.

157. Cong Cao et al., "Returning Scientists and the Emergence of China's Science System," *Science and Public Policy* 47, no. 2 (December 5, 2019): 172–83, https://doi.org/10.1093/scipol/scz056.

158. Vivek Wadhwa et al., "America's Loss Is the World's Gain: America's New Immigrant Entrepreneurs, Part IV," March 2009.

159. Vivek Wadhwa, "Why Skilled Immigrants Are Leaving the U.S.," *Bloomberg*, March 1, 2009.

160. Kevin Burns, "Essential Immigration Policy Reform: Reinventing the National Interest Waiver," *Akron Law Review* 53, no. 1 (2019): 246–74.

161. David R. Henderson, "Is China an Economic Threat?," Hoover Institution, August 27, 2020.

RELATED PUBLICATIONS FROM THE CATO INSTITUTE

Buying Lottery Tickets for Foreign Workers: Search-Cost Externalities Induced by H-1B Policy by Rishi Sharma and Chad Sparber, Research Briefs in Economic Policy no. 246 (January 13, 2021)

Lift the Ban? Initial Employment Restrictions and Refugee Labor Market Outcomes by Francesco Fasani, Tommaso Frattini, and Luigi Minale, Research Briefs in Economic Policy no. 241 (November 18, 2020)

Immigrants Do Not Negatively Affect the Economic Institutions of American States by Alex Nowrasteh and Andrew C. Forrester, Working Paper no. 61 (November 11, 2020)

Illegal Immigration and Crime in Texas by Alex Nowrasteh, Andrew C. Forrester, and Michelangelo Landgrave, Working Paper no. 60 (October 13, 2020)

How Do Restrictions on High-Skilled Immigration Affect Offshoring: Evidence from the H-1B Program by Britta Glennon, Research Briefs in Economic Policy no. 233 (September 23, 2020)

The Role of Mexican Immigration to the United States in Improved Workplace Safety for Natives by Marcus Dillender and Melissa McInerney, Research Briefs in Economic Policy no. 229 (August 26, 2020)

Democrats and Trade 2021: A Pro-Trade Policy for the Democratic Party by James Bacchus, Policy Analysis no. 900 (August 11, 2020)

How U.S. Travel Restrictions on China Affected the Spread of COVID-19 in the United States by Alex Nowrasteh and Andrew C. Forrester, Working Paper no. 58 (June 8, 2020)

12 New Immigration Ideas for the 21st Century by Alex Nowrasteh and David J. Bier, white paper (May 13, 2020)

Illegal Immigrant Incarceration Rates, 2010–2018: Demographics and Policy Implications by Michelangelo Landgrave and Alex Nowrasteh, Policy Analysis no. 890 (April 21, 2020)

Backlog for Skilled Immigrants Tops 1 Million: Over 200,000 Indians Could Die of Old Age While Awaiting Green Cards by David J. Bier, Immigration Research and Policy Brief no. 18 (April 7, 2020)

Border Walls and Crime: Evidence from the Secure Fence Act by Ryan Abman and Hisham Foad, Research Briefs in Economic Policy no. 207 (March 25, 2020)

H-2A Visas for Agriculture: The Complex Process for Farmers to Hire Agricultural Guest Worker by David J. Bier, Immigration Research and Policy Brief no. 17 (March 10, 2020)

Financing Immigration: The Financial-Market Value of a Market-Based Immigration System by Alex Nowrasteh and Andrew C. Forrester, Immigration Research and Policy Brief no. 16 (February 12, 2020)

Immigrant and Native Consumption of Means-Tested Welfare and Entitlement Benefits in 2016: Evidence from the Survey of Income and Program Participation by Tu Le and Alex Nowrasteh, Immigration Research and Policy Brief no. 15 (January 14, 2020)

Trust Doesn't Explain Regional U.S. Economic Development and Five Other Theoretical and Empirical Problems with the Trust Literature by Alex Nowrasteh and Andrew C. Forrester, Working Paper no. 57 (January 6, 2020)

Immigration Demand and the Boomerang of Deportation Policies by Christian Ambrosius and David Leblang, Research Briefs in Economic Policy no. 194 (December 18, 2019)

Immigrants Learn English: Immigrants' Language Acquisition Rates by Country of Origin and Demographics since 1900 by Michelangelo Landgrave, Immigration Research and Policy Brief no. 14 (September 17, 2019)

Legal Immigration Will Resolve America's Real Border Problems by David J. Bier, Policy Analysis no. 879 (August 20, 2019)

Do Immigrants Import Terrorism? by Andrew Forrester, Benjamin Powell, Alex Nowrasteh, and Michelangelo Landgrave, Working Paper no. 56 (July 31, 2019)

The Myth of the Cyber Offense: The Case for Restraint by Brandon Valeriano and Benjamin Jensen, Policy Analysis no. 862 (January 15, 2019)

A Balanced Threat Assessment of China's South China Sea Policy by Benjamin Herscovitch, Policy Analysis no. 820 (August 28, 2017)

CITATION

Nowrasteh, Alex. "Espionage, Espionage-Related Crimes, and Immigration: A Risk Analysis, 1990–2019," Policy Analysis no. 909, Cato Institute, Washington, DC, February 9, 2021. https://doi.org/10.36009/PA.909.