Recommendations to Address Government Concerns Regarding Intellectual Property Theft from American Research Universities by China and Other Foreign Entities while Preserving the Process of Fundamental Research

by

Jason E. Thomas, Ph.D., Alicia Wittkopf, Jonathan Dobbins, and Ronnie Rivera

Under the Supervision of

Dr. Kevin Gamache

Chief Research Security Officer

Texas A&M University System

Prepared for

The Association of American Universities

April 21, 2019

Texas A&M University

Table of Contents

Executive Summary

The United States government has identified intellectual capital loss and intellectual property theft of United States research universities by foreign entities as a critical problem. The federal government's response has been aggressive and thorough. Recommendations have been made to limit the ability of research teams comprising foreign researchers to work in government-funded research projects, as well as to reduce the budgets of the National Science Foundation and the National Institutes of Health. In addition to causing funding issues that could drive researchers to seek out other sources of research funding such as foreign entities, these recommendations could have lasting effects on an already-strained academic research system suffering from a lack of available research talent.

Currently, research universities depend on foreign graduate students to bolster the work and skill of research teams in the areas of science, technology, engineering, and math. The government recommendations to limit their impact, which are not without stimuli such as a growing number of recent cyber attack and intellectual property theft cases, contribute to the perception that foreign researchers and students are unwelcome in the United States. This perception exacerbates the shortage of science, technology, engineering, and math research talent for university research efforts, especially because of strong demand by the private sector to recruit these students and faculty members.

This report discusses and examines the factors surrounding this dilemma—government perspective, academic perspective, shortage of graduate research students, foreign entities identified as intellectual property risks, cyber security, funding, legislation, and policy. To create more appropriate and effective solutions, guidance is provided that reframes the issue as a security problem rather than a foreign-entity problem. The report makes 12 recommendations based on a best-practices survey of research teams from 39 premier research institutions to address the issue while preserving the concepts of fundamental research and academic freedom.

Introduction

The growing global economy is fueled by innovations in technology that depend on the development of intellectual property (IP)—making research, innovation, and the development of intellectual capital some of the most valuable activities in which organizations can invest. The United States (US) historically has been the global leader in innovation and research. However, this position now is being challenged by foreign entities, most notably China (Cimpanu 2018, Department of Defense 2018, Haas 2018, Posen 2018).

Many blame the potential loss of the US's economic position on the theft and loss of IP (Department of Defense 2018, Haas 2018, Halbert 2016). IP theft is a real problem. The US government has estimated that more than $600 billion in trade secrets was stolen from US organizations by foreign entities in a single year (The National Bureau of Asian Research 2017). Many suggest that China is fostering its mission to become the leading world economic power by IP theft (Cimpanu 2018, Haas 2018). Another component complicating the matter is that other nations (especially China) do not place the same value or emphasis on IP or its protection as does the US (Department of Defense 2018). These factors create a strong motive and vehicle for theft of US IP by other nations.

Government and business leaders have taken notice of these issues and now are calling for restrictions to protect intellectual capital developed in the US (Redden 2018). This reaction seems reasonable given the value and precious nature of these resources. The government's reaction has been firm and far-reaching, with calls to restrict government funding for research teams consisting of foreign students (Edwards 2016) and to cut the National Science Foundation's (NSF's) budget by $1 billion (Elis 2019). Both these actions exacerbate problems plaguing research efforts today—funding and a critical shortage of research talent.

It is important to ensure that actions taken to protect IP do not stifle the ability to share information and further scientific discovery and do not destroy the ability to create intellectual capital (Norris 2003). Put another way, we must ensure that the cure is not worse than the disease. To accomplish this goal, contributors and decision makers must acknowledge the problem and provide a thoughtful response about how to address these government security concerns while maintaining the ability to share information freely. This report explores the issues surrounding this problem and makes practical recommendations to address the government's security concerns while empowering the free exchange of information.

Background

The current challenge does not represent the first time that US IP has been threatened. During the Cold War, the US and the Soviet Union competed in the Space Race for spaceflight dominance. The Soviet Union took an early lead in this competition by launching Sputnik I and becoming the first country to put an artificial satellite into space. When this occurred, US leaders were shocked into action. The government's response to Sputnik I was to increase research efforts, create programs to increase educational opportunities, and empower Americans—all in support of driving scientific discovery (Homer, Smith and McCormick 2008).

Yet for the similar challenge faced currently, the response seems to be to diminish academic freedom and scientific research support rather than strengthen it (National Academies of Sciences, Engineering, and Medicine 2016), partly because of the nature of academia and the drive to share fundamental research. The momentum of knowledge sharing often means that US-based researchers can be ignorant regarding the intentions and reach of foreign challengers. "Many U.S.-based researchers are naïve to the methods and intent our foreign adversaries are using to gain access to our sensitive technology. The result is that they become unwitting participants in these talent platforms" (Gamache 2018, 1).

This is no longer the Cold War era, and the very nature of the problem is changed. Research and IP drive not only military efforts, but economic prosperity. The US is no longer necessarily the world leader in research and development (R&D); the US benefits from receiving information in collaboration just as much as other nations do. The world is becoming increasingly global, and universities are increasing the international diversity of their student populations. Research institutions engage these foreign students to bolster research teams. Foreign entities increasingly are funding research efforts and campus initiatives, creating a potential conflict of commitment. The issues surrounding this problem are complex, so prescribing a solution to address the problem proves complicated at best.

Problem Statement

This report addresses the problem of American research university intellectual capital loss and IP theft by foreign entities. The effects of IP theft are staggering. The US has suffered billions of dollars in economic losses due to IP theft, losses that are exacerbated by the specific danger of China surpassing the US as an economic power by growing its intellectual capital stores (Haas 2018). An update to the *IP Commission Report* estimated that losses due to IP theft are more than $225 billion in pirated software and counterfeit goods and as much as

$600 billion in theft of trade secrets (The National Bureau of Asian Research 2017).

The government's response to this problem, though, could have ramifications beyond the damages already suffered from IP theft—long-lasting consequences to academic research and the ability to share information freely, both of which drive innovation and scientific discovery. US lawmakers have identified American research universities as prime targets for IP theft by foreign entities. Several recent events bolster this perception: recent cyber attacks by Iran against 70 universities around the world (Osborne 2018), the National Bureau of Asian Research's report on IP theft designating specific foreign entities as likely cyber aggressors and identifying research institutions as prime targets for attack (The National Bureau of Asian Research 2017), and allegations of theft of US research by foreign entities such as China (Llorente 2019). One such example is that of Dr. Yiheng Percival Zhang, who is accused of fraud, having applied for and received funding in the US for research already conducted in China.

There are many other similar incidents contributing to the perception of significant IP theft and conflict of commitment on the part of foreign researchers. Consequently, the federal government is calling for strong measures to address this problem, such as more stringent screening of foreign students to hinder spies from gaining access to academic research facilities (Ross 2018). Lawmakers and government stakeholders are proposing greater security restrictions be placed on federally funded research projects that could be vital to national security (Edwards 2016).

The measures resulting from the government response to this problem could be extremely taxing to research universities, which are struggling on many levels already. If not properly addressed, this issue could have the following negative impacts on research institutions:

1. Exacerbation of research talent shortage—Currently, there is a dearth of research talent. US research institutions have sought to fill this void by attracting foreign research talent. Even though the concerns over IP theft are directed at a small percentage of bad actors, the actions and communications around this issue could contribute to the perception that foreign graduate students are no longer welcome in the US. Anecdotally, one major research institution has reported a 50% drop in foreign graduate applications for a hard science program (T. Smith, personal communication, March 7, 2019).
2. Reduction in government funding for research—Recently, statements have proposed a 13% budget reduction for the NSF and a 12% budget reduction for the National Institutes of Health (NIH) (Achenbach, et al. 2019), amounting to $1 billion and $4.5 billion lost, respectively. Both agencies are major funders of US research, and the effects of

these budget cuts could drive US researchers to work with other funding sources such as foreign entities.

3. Restrictions on the ability of foreign researchers to participate in government-funded research—Government officials have proposed restricting participation in government research projects based on research team composition (Edwards 2016). This measure could have far-reaching implications. Some universities or researchers might opt out of critical research initiatives, the government might eliminate the ability of some institutions to obtain federal research funding, and the lack of available research talent will be exacerbated further, which could cause the US to miss out on the opportunity to generate significant scientific discoveries.
4. Deincentivization of the academic science, technology, engineering, and math (STEM) workforce—Research institutions compete with the private sector for STEM talent, with recent graduates finding few incentives to take on research roles after earning their degrees. STEM graduates command some of the highest salaries in the job market, with starting average salaries ranging from $62,177 to $69,188 annually (Ascione 2019). In high-demand areas such as cyber security, first jobs could even earn as much as a six-figure salary. These numbers are contrasted with the choice to go on to graduate

> studies and contribute to research efforts, which incurs $50,000 to $100,000 in additional tuition costs and abandons two years of lost wages and career progression. Many opt to head for the private sector in the first place, and a mismanagement response to IP theft provides even more justification.

The response to this matter may have far-reaching consequences on the ability of US research institutions to conduct research. Fundamental research and the free exchange of information are the primary drivers for educating the workforce and generating scientific discoveries, and the system is already suffering from many challenges—further inhibiting this process could have drastic consequences for science and society (Homer, Smith and McCormick 2008, National Academies of Sciences, Engineering, and Medicine 2016). Accordingly, government concerns regarding this issue must be addressed quickly and comprehensively.

Purpose of the Study

The purposes of this study were to examine the potential threat of American intellectual capital loss and IP theft by foreign-entity interactions with American research universities and to provide recommendations to address government concerns. These aims were accomplished by conducting a systematic literature review, applying a risk management framework to examine the problem, and reviewing a survey of best practices for research institutions.

The information gathered in this study and the recommendations made in this report can be used by the American Association of Universities (AAU) and its member institutions to prepare responses to address issues regarding the growing threat of IP theft while preserving the principles of academic freedom and fundamental research.

Research Questions

Research questions for this study include the following:

Q1: How can potential threats to American intellectual capital be properly addressed while preserving the concept of fundamental research?

Q2: What are the inherent risks to academia actively engaging with foreign entities for activities such as recruitment, research, sponsorship, funding, academic collaboration, and student development?

Q3: How has the definition of intellectual capital changed and influenced this issue?

Methodology

The methodology used in this study was a systematic literature review, application of a risk management framework to examine the problem, and review of a best-practices survey of member institutions conducted by the AAU and the Association of Public and Land-Grant Universities (APLU).

Systematic Literature Review

Systematic literature reviews have been used extensively in social science research such as business, public administration, education, and information systems to gather facts and historical information about problems to be examined (Jesson, Mattheson and Lacey 2011, Kim 2018, Thomas and Hornsey 2014, Thomas 2017). The research team conducted thorough research utilizing university academic libraries, dedicated research tools such as EBSCO and ProQuest databases, and open Internet data sources such as Google Scholar. Keyword searches were used to identify materials of interest and included terms such as IP theft, intellectual capital, China, research university, and various combinations and delineations. This effort enabled the team to identify specific resources from the vast array of data that exist.

Risk Management Framework

A risk management framework from the cyber security domain was selected as a way to frame the problem. Cyber security is a growing concern for nearly all organizations (DHS 2015, Morgan 2017, Newman 2018, Thomas 2018). It seems that new stories of security breach resulting in exposure of personal and confidential information appear daily. Consequently, risk management and the ability to recover from cyber attacks are critical to maintaining ongoing operations and protecting vital data and IP (Harnedy 2016, Thomas and Galligher 2018). The recent surge of exposure from cyber attacks has forced many organizations around the world to focus on robust security practices to protect vital IP and intellectual capital.

The risk formula used for this study is as follows (Impe 2018):

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$$

This basic formula provided an intuitive method to help stakeholders conceptualize this complex problem. In looking at this formula, it became clear that substantial disagreement exists on the consequences of certain actions (limiting the open exchange of information) and the threat posed by the human talent on research teams, particularly those individuals foreign to the US.

ISACA®, a leading cyber security standards and certification organization that, for years, has set the standard for cyber security audits and compliance, recommends the risk management framework shown in Figure 1 to protect data and intellectual property.

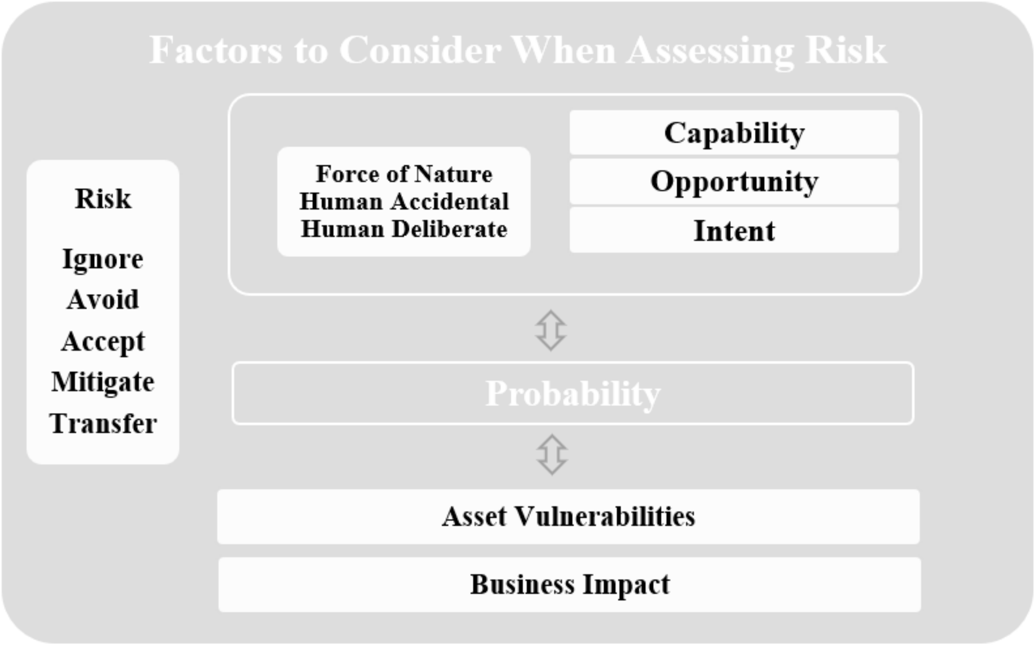


Figure 1. Risk assessment framework, adapted from (Gelbstein 2013).

This model was used as a lens through which to view the problem of intellectual capital loss and IP theft of American research universities by foreign entities. In the threat category, force of nature was excluded because it was not found to apply to the research problem. The team focused on human accidental threats and human deliberate threats.

Human accidental threats are those that result from unintentional behaviors such as being tricked to perform an action or being unaware that an action will have negative consequences (Gelbstein 2013). Generally, this type of threat is addressed by user education. For example, phishing is the most common vector for cyber attack (Aguilar 2015, PhishMe 2016, Thomas 2018). Phishing occurs when cyber attackers or other ill-meaning actors attempt to target an end-user with information that would lend credibility to the message or the request. An end-user might receive a message containing facts that are familiar to the user, or the sender of the message may be pretending to be a trusted source, such as a bank or organization to which the user belongs.

Human intentional threats refer to deliberate actions by humans to violate established rules and compromise security (Gelbstein 2013). In cyber security, this type is referred to as an “insider threat.” Insider threats are particularly dangerous because insiders have unfettered access to systems and information (Elifoglu, Abel and Taşseven 2018). The negative consequences resulting from an insider threat can be the result of a bad actor’s purposeful actions or when an insider is placed under duress or undue influence, such as bribery.

Using this risk management framework enabled the team to focus on the pivotal point of the problem—human interaction. As humans are the operative point of these exposures, either inside or outside the organization, it became clear to the research team that this is a security problem hinged on addressing unintentional and intentional human behavior to cause harm to the system or to steal IP.

Organizational Survey Results

The AAU and APLU have worked diligently to identify best practices for universities to protect research from threats such as IP theft, academic espionage, and efforts from foreign governments or other entities seeking to have undue influence on research institutions or to subvert the practice of core academic values such as scientific integrity and free speech (AAU & APLU 2019). The associations worked together to conduct the survey to identify effective practices, tools, policies, and resources used by member institutions to address foreign security threats. Data were gathered from 39 member institutions, with more than 140 examples of best practices shared. The research team reviewed a summary of this information, and items from the survey are detailed in the recommendations at the end of the report.

The Importance of Academic Freedom

The 1940 Statement of Principles on Academic Freedom and Tenure outlines the basic tenets of academic freedom. Among those tenets is the belief that pedagogical research is protected from undue outside influence. Faculty are free to conduct research on any given subject and publish the results without fear of consequence from the university (American Association of University Professors n.d.). This ideal establishes the concept of integrity within the American academic community that publication of the results of academic research is open to not only acclaim and potential use for applied research, but also criticism. One of the shared themes of concern among American research investigators is related to academic freedom abroad. For example, the Chinese government has been known to dictate research for its scientists and restrict the opportunity to conduct fundamental research that does not have specific implications for applied research aligned with their governmental goals (Suttmeier, Scientific American 2018). This example serves as just one reason why preserving academic freedom in the US is vital to its continued position as a world leader in scientific research.

The Importance of Fundamental Research

Fundamental or basic research is defined in US legal terms as "systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications towards processes or products in mind" (Cornell Law School n.d.). While the science of discovery is exciting, it also has many challenges. A decrease in funding fundamental research puts America's status as a leader in scientific knowledge at risk because fewer graduates pursue research as a career, and reduced funding makes it difficult to acquire the resources necessary to conduct basic research; yet basic research is necessary to develop new technology that has the potential to impact many sectors like defense, technology, and healthcare (Karagianis 2014).

The speed at which fundamental research can be conducted has continued to improve with the advent of technology. For example, the Internet makes it possible to find basic research that has been conducted on related concepts with a quick search engine inquiry, which can then be downloaded for review just as quickly. The open environment fosters curiosity and applied development research that seeks to address specific problems, which leads to commercialization opportunities (Remedios 2006). This connection was supported by a review of patents issued from 1976 to 2015 that were cross-referenced with more than 32 million scientific articles published after World War II; the review associated 80% of articles with at least one citation with future patents (Ahmadpoor 2017).

Information sharing is augmented by collaboration as well. Collaboration can resolve funding challenges, and, where geographical distance may have been difficult to overcome before the Internet, it can unite global field experts for the purpose of scientific inquiry without restriction. Significant debate exists on the effect of reduced funding for fundamental research, and what is available, some would argue, is not spread throughout the US in an equitable manner; therefore, state legislators have called for collaborative partnerships with international scientists and funding sources to pursue scientific research (Hoy 2018). These collaborative partnerships are well established in international countries like Japan, where research funding has continued to decline. In an effort to keep pace, Japan has accepted a partnership with China to open up new avenues of research that were not available previously because of budget constraints, as well as to yield higher-quality results from the information exchange between the two countries. Of the nearly 25,000 signed academic partnerships in Japan, 4,500 are with China and 3,187 are with the US (Kakuchi 2018). To understand the rate at which international scientific collaboration is accelerating, an evaluation of published research in six top-tier and four mid-tier journals found that international collaboration increased from 25% in 2000 to nearly 50% in 2015 (University of Michigan 2017).

The Government's Concerns

The importance of academic freedom is paramount to the integrity and credibility of US-based research institutions, but to understand the complexity of the problem facing American universities in today's competitive global environment, we also must examine the concerns of the primary funder of sponsored research in the US—the federal government. To put it in perspective, the NIH is a major funding source for university-based research. The research budget for the NIH is more than $37 billion, of which only 10% is earmarked for NIH research conducted in its own labs. The majority of NIH funding is awarded to more than 2,500 universities and other research facilities via a competitive process; more than 50,000 projects have been awarded (National Institutes of Health 2018). A statement released by the NIH director identified three primary concerns that need to be reinforced to limit vulnerability and susceptibility to theft among US research facilities (Collins 2018). These concerns, while identified specifically by the NIH, apply to all agencies that engage in government-sponsored research (NIH Advisory Committee to the Director 2018). The first concern relates to disclosure challenges.

For example, often physicians at academic health centers are on staff or provide consulting services to drug companies. As it currently stands, anyone participating in research sponsored by government funding sources like the NIH is required to disclose their income and stock ownership related to activity like consulting services to pharmaceutical companies to limit conflicts of interest. In a federal investigation, authorities found that principal investigators requesting federal funding were engaged in fraudulent reporting of income or simply were not complying with the Public Health Service regulation that requires them to disclose any income exceeding $10,000 or 5% ownership (Kaiser 2008).

These disclosures also are required where foreign entities are concerned. Some investigators do not disclose that they receive resources, whether outright financial support for equipment and/or paid faculty and support staff, from foreign sources or entities with competing interests (NIH Advisory Committee to the Director 2018). As the old saying goes, “He who has the gold makes the rules.” As such, the government has cause for concern where universities don’t fully disclose all of their financial relationships because the integrity of the research could be compromised by outside funding sources causing undue influence. For example, a survey of academic health center faculty concluded that increased pressure on faculty to raise their own money to support additional research, salaries, and operations leads to misbehavior. Responses indicated that federally funded researchers are likely to engage in one misbehavior, while privately funded scientists are likely to engage in two or more misbehaviors, with the severity of their offenses being higher. Those whose livelihood or academic survival depends on raising their own capital are more likely to engage in misbehaviors because they have the most to lose (Martinson, et al. 2009). Thus, we can infer that researchers who also are sponsored or employed by foreign entities in some capacity are more likely to be subject to undue influence compared to peers who are not sponsored by foreign sources.

Further, faculty and support staff being funded by outside sources may create security breaches in the IP being funded by US-based governmental agencies (Collins 2018). An example of this is the Chinese talent recruitment program called Thousand Talents. The Chinese government sponsors students who have the ability to attain highly prized US-based research posts for the purpose of acquiring IP that then is disclosed to the Chinese government (Facher 2018). In some cases, the Chinese government also has been known to create shadow labs in China that resemble and work in sync with the information given to them by the Chinese-supported talent pool (Facher 2018).

One well-documented case of this type is that of the “invisibility cloak” led by Duke University principal investigator Dr. David Smith. Smith hired student and Chinese national Liu Ruopeng to work on a project using metamaterials to make items invisible to object-detecting equipment. Naturally, because of the defensive implications of materials that can go undetected, the Department of Defense was a major sponsor of Smith's work. Later, Dr. Smith learned that Ruopeng's friends took pictures of his lab and recreated the project in their lab in China. Ruopeng marketed the material for monetary gain; he is now worth an estimated $2.7 billion (McLaughlin 2018, Reisch 2018).

The last concern outlined by the NIH director is the vulnerability of the peer review process (Collins 2018). The NIH and other agencies have learned of several breaches in the peer review process leading to foreign entities obtaining confidential information documented in grant proposals (NIH Advisory Committee to the Director 2018). Those breaches have undermined the peer review process for US funding agencies and needlessly have exposed IP in grant proposals to foreign entities with the intent to exploit it for their gain. While the NIH is leading the charge on addressing these challenges, it is not the only governmental funding source that is subject to these concerns (NIH Advisory Committee to the Director 2018). Moreover, China is not the only foreign entity pursuing IP theft via US-based research. Russia and Iran have been identified as top threats to national security because they have extracted IP from more than 140 US universities (Riggi 2018). They also have hacked the email accounts of approximately 8,000 university personnel across the US, an act that rewarded them with 35 billion pages of research worth approximately $3.4 billion (Reisch 2018).

Foreign Intellectual Property Theft

IP theft is an expensive problem. In an update to the *IP Commission Report*, it was estimated that losses due to IP theft are more than $225 billion annually from pirated software and counterfeit goods and as much as $600 billion annually due to theft of trade secrets (Ackerman 2018, The National Bureau of Asian Research 2017). US lawmakers have identified American universities as prime targets for intellectual capital theft by foreign entities, calling for more stringent screening of foreign students to hinder those with mal intent from gaining access to academic research facilities (Ross 2018); however, there are no specific distinctions within the *IP Commission Report* that specify estimates of loss among sectors, which may indicate some misaligned speculation among legislators in naming higher education as the primary target for IP theft. Yet the Federal Bureau of Investigation (FBI) has warned that foreign spies are already active in American universities in all 50 states and that they have earned the confidence of their colleagues, thereby making them virtually undetectable. At a meeting in Houston, the FBI, along with Texas academic and research institution leaders, discussed the rapidly evolving threat of academic espionage in an effort to collaborate and find solutions that work to enforce the law while preserving the tenets of academic freedom (Ackerman 2018).

While some advocate for limiting the number of international students on campuses because of the risk of theft, this solution comes with a cost, too. Many professors agree that most international students come to the US with good motives and that restricting their admission could have dire consequences on the free exchange of ideas and scientific pursuits (Reisch 2018). Limiting the number of international students on campuses across the US also could have severe financial consequences for universities, their domestic students, and the US economy.

Because international students are not eligible for in-state tuition, their fees subsidize those of their in-state peers. In 2015, foreign students comprised 12% of the student population in public universities; yet 28% of the revenue at those same institutions came from that small population. Seventy-two percent of the international student population pays for tuition with support from one or more of the following sources: university assistance, home country sponsorship, family finances, or personal finances. Further, international student enrollment has been credited with adding $30 billion to the US economy in the 2015 academic year (Loudenback 2016). If universities were to lose international student revenue, they would be forced to pass on that cost to domestic students.

Another implication of IP theft is the active and ongoing evaluation of academic visas for students. Currently, President Trump is seeking counsel on restricting academic visas specifically for Chinese students in an effort to mitigate academic IP theft (Ambrose 2018). Because China is well known for cyber breaches that have resulted in the theft of IP (Barhat 2018) and because lawmakers and governmental stakeholders are proposing greater security restrictions on federally funded research projects that could be vital to national security, restrictions on academic visas may be closer than anyone realizes.

Currently, the Department of Homeland Security oversees the Student and Exchange Visitor Program (SEVP). The SEVP uses the Student and Exchange Visitor Information System (SEVIS) database to monitor any international student's eligibility to be admitted as a foreign student; data are accessed by universities attended by the student to notify the institution of any restrictions or requirements related to their academic visa (Department of Homeland Security 2018). The F-1 visa, which stipulates that a student must intend to return home upon graduation, is the most widely applied for and issued academic visa. A foreign student applies for an academic visa via the US Embassy in the country of their residence. Upon doing so, the student must provide documentation of finances, family, and prospective job offers that would exist following achievement of their degree (International Student 2019).

According to Dr. Kevin Gamache, Chief Research Security Officer for the Texas A&M University System, visa officers spend approximately three minutes reviewing visa applications and the documentation that accompanies them (K. Gamache, personal communication, March 7, 2019). When an international student applies for an academic visa, allotting an appropriate amount of time to vet the application thoroughly and trace the financial support of the student can eliminate bad actors before they are admitted to study in the US.

Should the pendulum swing too far and the restrictions on academic visas become too costly or difficult to overcome, combatting the IP theft problem in this manner at research universities would prove challenging because it endangers foundational scholarly precepts such as fundamental research and academic freedom (Edwards 2016), which may affect adversely the willingness of some institutions to participate in government-funded research initiatives.

The relationship between university research programs and the federal government continues to evolve, but it has been based on the tenets of academic freedom. As such, fundamental research has been the primary driver for educating the workforce and generating scientific discoveries; disturbing this relationship, even in the name of national security, could have drastic consequences for science and society (Homer, Smith and McCormick 2008, National Academies of Sciences, Engineering, and Medicine 2016).

Funding

Prior to World War II, industry funded most university research (Atkinson 2018). However, during World War II, the US government took strategic interest in funding and supporting scientific research at universities. After the successful Soviet Union launch of Sputnik I, American leadership came to the realization that the US was on the verge of being surpassed by its nearest rival and responded by increasing its focus on research universities to maintain its world position as the leader in scientific discovery (Homer, Smith and McCormick 2008).

Basic research accounted for 64% of university research in 2012. Of the $75 billion in funding for basic research in 2012, the federal government supported 52.6% of those dollars, down from its peak of 70.3% in the 1970s. In 2012, universities performed the largest portion of basic research across all entities at 53.5%. At its peak, the federal government was the largest supporter of basic research at universities in 1965 at 77.3%. In 2012, that share had declined to 60.7%. In the same timeframe, universities bridged the gap in the decline by allocating more of their own budgets to support basic research from 7.1% to 21% (Association of American Universities 2015). Table 1 shows federal funding of basic research by agency.

Table 1

Federal Research Funding by Agency (from AAU [2015])

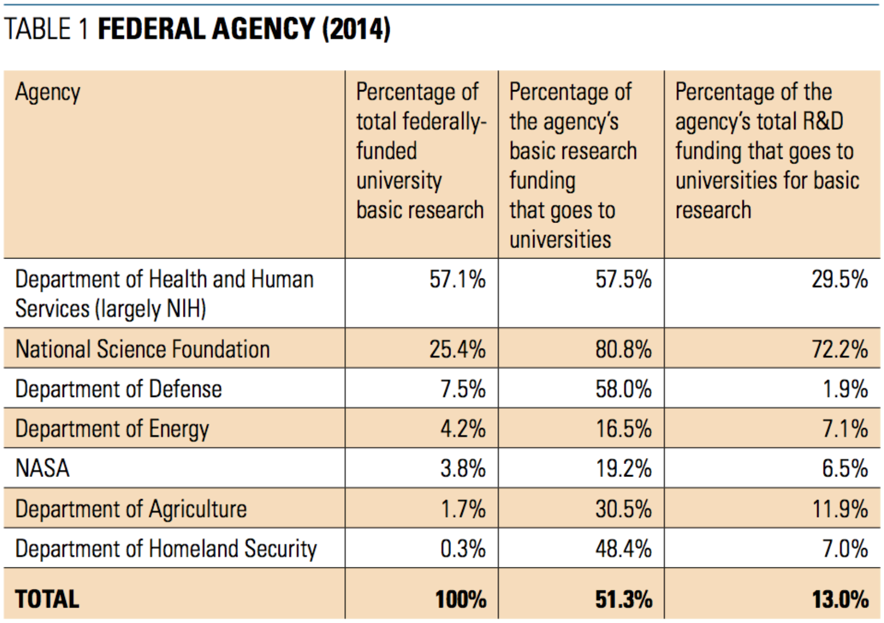


TABLE 1 **FEDERAL AGENCY (2014)**

Agency	Percentage of total federally-funded university basic research	Percentage of the agency's basic research funding that goes to universities	Percentage of the agency's total R&D funding that goes to universities for basic research
Department of Health and Human Services (largely NIH)	57.1%	57.5%	29.5%
National Science Foundation	25.4%	80.8%	72.2%
Department of Defense	7.5%	58.0%	1.9%
Department of Energy	4.2%	16.5%	7.1%
NASA	3.8%	19.2%	6.5%
Department of Agriculture	1.7%	30.5%	11.9%
Department of Homeland Security	0.3%	48.4%	7.0%
TOTAL	**100%**	**51.3%**	**13.0%**

Federal support for basic research accounted for 63% of the $71.8 billion spent in 2016 (The National Science Foundation 2018). In 2015, the total spend on all types of research was $499 billion, of which approximately one-sixth was basic research. The bulk of the spend was $316 billion for development, mostly performed outside of higher education with private firms looking to increase their bottom line (Mervis 2017).

R&D is big business in the US. As of 2015, the US led the world in expenditures on R&D at nearly $497 billion, or 2.7% of its gross domestic product (GDP) (Showstack, EOS Earth & Space Science News 2018). R&D funding for universities peaked at 73% in the late 1960s. Following its peak, it slowly declined and currently hovers near the 60% mark, although funding for higher-education institutional research has remained flat since 2005. The business share of R&D support has increased from 3% to 6% since the 1960s, and universities are increasing their subsidies of R&D as well from 10% to more than 30% in the same timeframe. The NSF has stated that more than $55 billion in R&D is conducted by colleges and universities annually (American Association for the Advancement of Science n.d.). In 2016, institutions of higher education spent $71.8 billion on R&D, 94% of which was spent on science and engineering endeavors. University expenditures on each of the NSF classifications of research—basic, applied, and developmental—were 63%, 28%, and 9%, respectively. Approximately 44% of all expenses were attributed to the human capital necessary to conduct research. Direct and indirect costs of conducting research accounted for the other 56%. While federal support has been declining, it is still a primary source of funding for academic research, accounting for about 60% of academic funding, while approximately 25% comes from the institutions themselves. The government spent $38.8 billion on funding R&D for universities and colleges in 2016; 90% of this funding came from six federal agencies: Department of Health and Human Services ($53.3 billion), Department of Defense ($13.7 billion), NSF ($13.2 billion), Department of Energy ($4.6 billion), National Aeronautics and Space Administration ($3.8 billion), and Department of Agriculture ($3.1 billion) (National Science Board 2018).

Following World War II, the US became the world leader in R&D by funding 69% of all R&D worldwide. Since other countries began funding R&D in 1953, the US has accounted for 28% of worldwide R&D funding as recently as 2015. The federal government and business have provided the lion's share (more than 90%) of R&D funding since 1953. In 1964, the federal government was the largest source of subsidy for R&D at 66.8%, and business was the lowest at nearly 31%. Since then, the roles of R&D share have reversed, with business being the primary source of R&D funding at 69.4% and the federal government at 25.1% in 2000. In 2015, the largest portion of funding for basic research, 44.3%, came from the federal government, while business was the largest subsidizer of applied, 53.3%, and developmental, 82.3%, research. Of those funding sources, 49.1% of basic research, 18% of applied research, and 2% of developmental research was performed by institutions of higher education (Sargent Jr. 2018).

While the US has been the world leader in R&D since World War II, there are major issues at play that may unseat America from the top spot. The primary issues threatening to remove the US as the world's research superpower are reductions to the federal budget that underwrite academic research and Chinese policies and investments in strategic initiatives like Thousand Talents, Made in

China by 2025, and World Leader in Artificial Intelligence by 2030 (Guarino, Rauhala and Wan 2018).

While the 2018 federal budget for the Department of Defense as related to the research component was increased by $865 million compared to the previous year, the bulk of the increase was earmarked for applied R&D (Hampson 2018). Department of Defense budget requests for 2019 have been met with opposition to increased funding for research, development, testing, and evaluation across all sectors of the armed forces and for the Defense Advanced Research Projects Agency (DARPA). In fact, when compared to the 2018 budget, nearly every major project or initiative, as well as those for each type of research across the spectrum, was assigned significantly less money in the 2019 budget. The single largest reduction was a 31.02% decrease to applied research for the US Army (Association of American Universities 2018). Later budget ratifications did include across-the-board decreases in all Department of Defense sectors except DARPA, which received a small increase in the applied and advanced technology budget for research (Hourihan 2018).

Agencies like the NIH and the NSF fund research out of discretionary budgets. A reduction to those budgets means removing funding from one program to fund research, which seems unlikely given that their budgets are consistently flat or reduced. Researchers have been successful at obtaining funding from the NIH and the NSF slightly less that one out of every five times, meaning that researchers must seek other funding opportunities and that many research projects cannot be maintained, certainly not to the extent and duration required to fund long-term research (Howard 2013).

Further, a proposed 20% cut to the NIH budget could have implications not just for higher-education research, but also for economic development, a conclusion based on a review of more than 365,000 grants awarded by the NIH from 1980 to 2007 that found 8.4% of awards to be directly responsible for US patents and more than 31% of grants to lead to research cited by other patents (Hampson 2018). Reducing the funding dedicated to biomedical research as supported by the NIH is a significant threat to the US position as a leading authority in scientific biomedical research (University of Michigan 2017). The federal budget is not something that is easily agreed upon; therefore, it is imperative that bipartisan support of federally sponsored research is not neglected.

As outlined above, cuts to federal budgets and difficulty obtaining and retaining grant funding for ongoing research proposals create many challenges in American academia because they give China the opportunity to recruit the brightest American minds to study in China, where incentives are many and where ongoing research funding is guaranteed. Highly regarded scientists are moving labs from Ivy League schools to China because of generous sign-on bonuses, high pay, world-class lab facilities, well-trained staff, and guarantees of continued funding, as well as other fringe benefits for family members (Guarino, Rauhala and Wan 2018).

The Chinese government has had trouble with some of its own laws regarding recruitment of these American researchers. For example, recruiting has been held up in the bureaucratic process until a Chinese-born collaborator has been found to partner with the recruit. As such, the Chinese State Administration of Foreign Experts Affairs (SAFEA) was moved to become a department of the Ministry of Science and Technology (MOST). The theory behind the move was to make it easier for foreign scientists to be granted the right to work in China. The SAFEA department oversees the Foreign Expert Recruitment Scheme, as well as the Thousand Talents program. A Duke University biologist serving as an advisor to the Chinese government for talent initiatives has made it clear that recruitment of foreign scientists to China is possible because funding in the US is on the decline. Moving SAFEA to the oversight of MOST removed some of the barriers preventing recruitment, like partnering with a Chinese-born collaborator. The ministry also is poised better to fast-track foreign experts who can fill high-need positions (Jia 2018, Kenderdine 2017). However, some Chinese researchers are concerned that the reorganization will make governmental initiatives a top priority instead of scientific inquiry leading the process; bureaucracy will and could consequently damage credibility of Chinese-led research. The Chinese government maintains this move as strengthening their position, not compromising it, and they will continue to work to promote international collaboration free from governmental requirements to pursue one type of research over another (Sharma 2018).

China's strong financial commitment to R&D has enabled the country to become a global leader in research (American Association for the Advancement of Science n.d.). China has increased its investment in research as a percentage of its GDP from 0.9% in 2000 to 2.0% in 2015, with a goal of 2.5% by 2020. It is ranked second to the US in R&D expenditures at 20% of the world total. Further, China is now second to the US in the number of doctoral degrees in science and engineering (Gupta and Wang 2016). For comparison, while the US continues to fund R&D and increased its allocations by an average of 4% each year from 2000 to 2015, China has had an average 18% growth year over year in funding R&D (Guarino, Rauhala and Wan 2018).

To date, the US has led the world in R&D expenditures. As much as 37% of global R&D was attributed to the US in 2000, but the number fell to 26% in 2015. China's total increased to 21% in the same timeframe. As of 2015, China became second to the US in R&D expenses, beating out the European Union, which is now third in R&D expenses globally (Showstack, EOS Earth & Space Science News 2018). While the US is regarded as the global scientific research leader, this regard is not likely to hold, as China is set to outpace the US in R&D expenses by 2022 (University of Michigan 2017).

Since 2014, the Chinese government has worked on a financial restructuring plan for the purpose of rapidly expanding R&D expenditures. The plan includes redirecting local funds to approximately 1,000 industrial development investment funds that total the equivalent of $500 billion. The Chinese government also has mandated that state-owned enterprises are required to redirect 1.5% of revenue to R&D, further increasing the funding available for R&D projects (Kenderdine 2017). In 2017, 77% of China's spend on R&D was allocated from Chinese enterprise (South China Morning Post 2018), indicating that mandatory R&D allocations by enterprise have been beneficial for the country.

While the Chinese are making advances that would lead competing nations to think that the country soon will be the global leader of scientific research, concern still exists among the academic community, some arguing that China's research lacks the depth and rich history of scientific leadership (Barhat 2018) and that issues still exist within Chinese-sponsored research that need to be addressed. Ethical concerns top the list because China does not have a regulatory system like the US to prevent the abuse of human subjects, which could discredit research. Additionally, the Chinese government has been known to impose quotas for published articles, which has led to several hundred articles being discredited for poor quality (Guarino, Rauhala and Wan 2018). While the Chinese have been able to invest substantial sums of money in R&D, some argue that for all the expense and effort, the result is not as grand as the Chinese would like. From 2010 to 2015, only 2.2% of US patents were issued to Chinese-based applicants compared to 18.8% from Japan and 5.5% from both Germany and South Korea. Further, China does not have a single university on the list of top 30 global universities cited in scientific journals (Gupta and Wang 2016). In many communities, the underlying concern about Chinese research is that objectives are dictated by the state government, which can feel restrictive to scientists and can hinder organic scientific developments. As time passes and China's R&D expenditures surpass those of the US, it will be of significant importance to observe how China manages the ethical dilemmas of driving science based on governmental objectives (Suttmeier 2018).

Issues Affecting the Intellectual Property Theft Problem

The Disappearing American Graduate Student

American universities have large populations of international students. More than one million international students are enrolled currently in higher-education programs in the US. Approximately 5% of all students enrolled in higher education in America are international students (Leiber 2018). These numbers show a substantial increase from foreign student enrollment in the 1950s, which was estimated at approximately 35,000.

A report by Lieber (2018) outlined the need to attract foreign talent to work in American research programs. While many countries offer grants and assistance for students wishing to study in the US, students must be accepted into American institutions before they can quality for these assistance programs. Further, students must be accepted into American education institutions before they can apply for student visas (Leiber 2018). Lieber's (2018) report also suggested that it is difficult for foreign student to obtain work visas in the US. Many business schools inform prospective international students about the challenges of obtaining employment in America as part of their orientation programming.

Foreign-student applications to American universities dropped 11% in 2018, according to a survey of 400 US institutions offering graduate business programs (Leiber 2018). Some 47% of non-US students considering Master of Business Administration (MBA) programs outside of their home countries favor American research institutions as their first choice for attendance, a 9% drop from the same survey conducted in 2016 (Leiber 2018). This decline raises concern for American research institutions, which already are suffering from a lack of graduate research talent.

The value of global exchange students.

Failing to engage foreign graduate students could undermine significantly the ability of American research universities to innovate, develop programs to generate intellectual capital, and create IP. IP laws vary globally. China, for example, asserts that all IP belongs to the government. These views seem to be based philosophically on Confucianism (Alford 1997). Confucian traditions do not place value on individual property rights. These radically different views on IP rights create an inherent conflict between western nations and China. Historically, there have been two attempts to reform Chinese copyright laws at the beginning and end of the 20th century. Both attempts failed. These philosophical issues are the foundation for the government's concern with foreign graduate students.

Research Talent Shortage

The preconceived notion of a shortage of scientific investigators has been a topic of conversation for decades, with data suggesting that the US is meeting the demand of graduating advanced-degree holders in STEM fields (Greenberg 2003, Weeks 2015). The challenge is not the number of graduates, but the desire of those graduates to choose to enter the research sector; overwhelmingly, they do not. The lack of interest in entering a postdoctoral career in research is attributed to two factors: the length of time it takes to secure a postdoctoral appointment and the meager salary paid for the work (Greenberg 2003).

Since World War II, the US has been tremendously successful in recruiting foreign-born scientists for US-based research activity; however, the nation is now losing ground because other countries are putting salary and other incentives on the line for the best talent to join their ranks in the realm of research (Guarino, Rauhala and Wan 2018, Gupta and Wang 2016, Weeks 2015). China, for example, is funding the recruitment of talented scientists more successfully compared to its primary competitor, the US. China is attracting bright minds by funding large-scale science projects like the world's largest radio telescope and massive particle accelerators.

China also has amended its policies so that foreign researchers are allowed to lead Chinese public research projects. Further, more and more elite scientists are moving to China to conduct their research because of large paychecks and ongoing funding agreements. Scientists say that language and access to resources like Google are drawbacks, but the benefits outweigh the challenges, which are not insurmountable (Normile 2018).

Research talent and hard science skills are sought after highly. Computer scientists are in high demand, not only in academia, but also in the private sector, which offers higher salaries and strong benefits programs (Greenberg 2003, Metz 2018, Weeks 2015). There is a national shortage of computer science faculty because these individuals can enter private industry and make, on average, five times the salary of a tenure-track professor. This challenge has had tremendous consequences for many universities with computer science programs, including limiting the number of computer science majors and eliminating it altogether at liberal arts universities, thereby putting additional burden on the small pool of computer science faculty remaining in the education sector (Flaherty 2018).

Cyber Security

One hardly can turn on the daily news without hearing about new cyber incidents or cyber crimes. While much of the population (and certainly much of the faculty at research institutions) is aware of the growing problem of cyber security, individuals may not be aware of the significant scale of the problem and the substantial effort and expense expended to address the problem (Wilday 2018). Because we are inundated with reports of cyber incidents on a daily basis, people simply may have become accustomed to the fact that a cyber problem exists; this numbness might cause one to assume that the problem is an acceptable fact or that it is being solved properly already.

However, the scale of the problem makes it a truly cataclysmic issue. Cyber criminals conduct cyber crimes for the most basic of human motives—profit. There is no doubt that cyber crime is profitable. Experts currently estimate cyber crime as generating at least $1.5 trillion in revenue each year (McGuire 2018). Table 2 breaks down that total.

Table 2

Breakdown of Cyber Crime Revenue (Adapted from McGuire [2018])

Cybercrime	**Revenue per Year**
Illicit/illegal markets online	$860 billion
IP/trade secret theft	$500 billion
Crime-as-a-service/crimeware	$1.6 billion

Ransomware/extortion-based malware	$1 billion

This total—$1.5 trillion—is a tremendous amount of money. To put it in context, if cyber crime were a nation-state, it would have the 13th-largest GDP, pushing Australia to number 14 on the global list of top 20 exporters (Prableen 2019).

Ransomware has been in the news for the past few years and has become a topic discussed by many. However, as can be seen from Table 2, the billion-dollar ransomware problem is less than one-twentieth of 1% of the value of IP theft to a potential cyber miscreant. This makes research universities huge targets (Gamache, Senator Cornyn questions for the record for Dr. Kevin Gamache, Chief Security Officer, Texas A&M University System 2018, Halbert 2016, Ross 2018, Saady 2018, Timmons 2018).

While a full discussion of the dangers inherent to cyber attacks and the need for a conference of cyber security is beyond the scope of this report, two points are extremely important when discussing the protection of intellectual capital and IP theft from research universities: insider threats and advanced persistent threats.

Insider threats.

In a survey conducted by CA Technologies, more than 90% of organizations reported feeling vulnerable to insider attack (Schultze 2018). An insider threat can be defined as a threat that comes from a person or people inside the organization. While most think of this concept as an insider with malicious intent, insider threats can come from employees and other people with access who *unintentionally* threaten the organization.

Individual users are the most common vector for cyber security attack (Schultze 2018, Thomas 2018). Often, cyber attackers gain access to computer systems by means of phishing or spear phishing (Nihco, Fakhry and Uche 2018). Phishing is the process of sending emails to users with links they can click on that will either spread malware or viruses or attempt to gain information from the user that can be used to compromise systems, such as a fake bank login. Spear phishing is a more targeted form of phishing where the message is populated with information familiar to the user to encourage them more powerfully to interact with the trap.

Once these users become compromised, the high level of access that they have within the organization, coupled with the multiple number of devices on which they may have access to sensitive data, becomes an extreme challenge for security (Schultze 2018). If given access, the miscreant essentially can act as the user, either to insert malware or trapdoors that let in others or to access data with which the user is entitled to interact. Both of these options are strong enablers for IP theft.

In order to combat this issue, organizations are taking proactive measures such as user training and awareness, deterrence methods, and behavioral-monitoring methods for both data and users (Schultze 2018). Popular tools to implement these methods include data loss prevention, encryption and identity verification, and access management solutions.

Another type of insider threat is that of a malicious bad actor. While 51% of companies surveyed expressed concern over accidental or unintentional insider threats such as carelessness, compromised credentials, or negligence; 47% of companies expressed concern over threats from insiders who would cause harm deliberately (Schultze 2018).

Insider attacks are real and occur frequently; 33% of organizations have experienced 1 to 5 insider threat–based cyber attacks in the past 12 months (Schultze 2018). Some 73% of companies perceive that insider attacks continue to occur at the same or more frequent levels. The possibility of foreign researchers acting as negative insider threats is one of the greater concerns of the government and other interested stakeholders (Gamache 2018, Grassley 2018).

In addition to profit motives for the individual, there are much larger and complex pressures that could come to bear on foreign students working on US-based research teams (Cimpanu 2018, Demchak and Shavitt 2018, Department of

Defense 2018, Edwards 2016, Lawder 2016, Shoebridge 2018). For example, countries such as China have specific goals to develop and acquire IP and often have been accused of stealing IP. A given product of research could prove valuable for its owner, which is one of many reasons why one entity would want to obtain research developments from another.

When foreign entities have students inside US universities, these students could feel pressure to act in certain ways to further the interests of their host countries. The pressure could vary from something simple like national pride and support of one's country to something more specific—negative pressures like threats against a student's family or positive threats like obtaining status and financial gain upon returning home.

Advanced persistent threats.

Advanced persistent threats (APTs) pose great danger to American research institutions (an example is the Iran hacking incident discussed in detail later in the reprot). APTs are cyber attackers who initiate attacks using several different techniques and vectors conducted by stealth over time to avoid detection (Tankard 2011, Li, et al. 2018). This type of attack allows deep and wide-ranging access to computer systems and organizations. Information can be stolen over long periods and go undetected. The cyber attackers also can place hooks into the environment that are very difficult to remove during a specific attack (or ever).

Because of the complex and compromising nature of APTs, they require substantial skill, expertise, resources, and manpower to conduct. As such, most APTs are thought to be sponsored by nation-states such as Vietnam, South Korea, China, Russia, Iran, and others, as well as by criminal organizations (FireEye 2019). Experts believe that the recent attacks by Iran targeting the IP of educational institutions and universities from 14 countries were conducted by the APT group known as Cobalt Dickens (Osborne 2018).

Cobalt Dickens is thought to have stolen information from 76 universities in 21 countries, 47 private companies in the US, the US Department of Labor, and the United Nations (Osborne 2018). The most recent wave of attacks targeted 76 universities from 14 countries, Canada, China, Switzerland, the United Kingdom, and the US being among them. Universities were sent phishing emails containing fraudulent domains; when the users clicked on these domains—making this an example of an insider threat—the cyber attackers gained access to target systems (Osborne 2018). This recent example illustrates just how pervasive APTs are and how dangerous they can be to universities or other prime targets with valuable research.

Foreign Entities

Countries around the world are rapidly coming to the realization that IP and innovation are the political currency of the new technology-based economy. These assets and abilities affect most major domains such as economic viability, effective governance, and military prowess. This situation creates a complex relationship with foreign entities looking to increase their intellectual capital through research and study within a university education system that promotes the open exchange of information on a global scale.

China.

The Chinese Communist Party's Central Committee has placed a high priority on education and technical innovation as a means to establish a strong place on the world stage. The warlord Yen Hsi-shan attempted to modernize the weak Chinese economy in his province by carrying out the Ten-Year Plan of Economic Reconstruction (Gillin 1965). Yen's outline for promoting economic growth in Shansi, China's First Five-Year Plan, was inspired by the success of Stalin's first Five-Year Plan for the Soviet Union (Gillin 1965).

China's first Ten-Year Plan attempted to reduce the autonomy commonly enjoyed by local officials in Shansi through economic controls created by the reinforced determination to concentrate authority in the hands of a Chinese warlord. Soviet successes caused Yen to become acutely conscious of the immense power possible if China's vast population were liberated together as a unified people. It not only caused him to overlook the economic interests of the rich, but also demonstrates why he tried to educate the masses and urged them to engage more actively in economic affairs. Yen's determination to build an industrialized power-state exceeded both his ambition for the state's participation and his anxiety over a social or economic revolution.

Confucian centers.

The Chinese government invests heavily in talent programs aiming to attract educators and principal experts in the west. The growing controversy concerning Confucius Institutes in the broader political space transcends the ideological conflicts that have fostered the question of what Confucius Institutes advocate and how they influence those who learn Chinese language and culture all over the world (Hartig 2015). The Confucius Institute program began in 2004 led by the Office of Chinese Language Council International (Hartig 2015). The institutes operate in cooperation with local affiliate colleges and universities around the world and are financed between Confucius Institute headquarters and the host institutions.

The stated goal of Confucius Institutes is the promotion of nonprofit educational organizations to teach the Chinese language outside China. The program has been successful and is growing (Tang 2010). By December 2014, there were 475 Confucius Institutes and 851 Confucius Classrooms in primary and secondary schools in 126 countries (Sun and Cheng 2014). There are also more than 200 institutions in some 70 countries currently applying to have a Confucius Institute (Liu 2014).

All Confucius Institutes are under the supervision of Hanban, the headquarters for the Office of Chinese Language Council International. Hanban is responsible for institute administration, teacher supply, and development and distribution of teaching materials. Although Confucius Institutes were located initially in colleges and universities only, in 2007 Hanban launched the Confucius Classroom program, a Chinese language and culture program similar to Confucius Institutes, but located in high schools. Usually, the Chinese supply teaching materials and send over language teachers, while local partners provide accommodation, facilities, and local staff. The host institutions typically receive initial funding of $100,000 to $150,000 per educational hub for a period of three to five years.

Five-Year Plans in connection to education.

With the birth of a new China in 1949, Mao Zedong chose to lead the country on a path toward Maoism. Based on a Maoist model of expansion, China's socialism produced a fundamentally different governmental organization and a new socioeconomic guide called the First Five-Year Plan (1953 to 1957). This change was demonstrated best by the urban transformation of Hangzhou between 1949 and 1978. The city of Hangzhou's urban transformation from 1949 to 1978 provides an understanding of the urban economy, population management, and city-planning ordinances of the First Five-Year Plan (Qian 2015).

The plan prioritized for China the Soviet Union's development paradigm of industrialization over other forms of economic models (Qian 2015). The plan exhibited how essential it is to strengthen the labor market in order to transform from a consumption center into a production center. For Hangzhou, the First Five-Year Plan dramatically restructured the city's economic sectors from 1953 to 1957.

The Second Five-Year Plan (1958 to 1962) brought economic adjustment for Hangzhou to set its goal of being a large industrial city. This adjustment unavoidably resulted in urban policy inconsistency and a disparity between ideology and practice influenced by the political agenda of the first two Five-Year Plans (Qian 2015). In order to maintain its power and domination solidly, the communist state installed spatial preconditions of surveillance and control of people's daily actions through political ideologies such as collectivism, population management of youth rustication, and physical specifications of an urban commune, self-contained neighborhoods, and Soviet-style planning and design. The realization of Mao's ideal socialist culture during this period prevailed upon the collective interest instead of the private interest and at the expense of individual urban citizens (Qian 2015).

Fast-forward to the Ninth Five-Year Plan, in which national economic and social development are stressed and science and technology are the first forces of production and education for the nation's foundation. The plan provides modernization for the Chinese that can be achieved only through sound educational practices that apply to increasing the spirit of the nation in all fields of endeavor. This plan holds science and technology as centers of modernization for the Chinese to increase educational practices in all fields of endeavor. China's Communist Party has implemented all types of strategies to ensure increased labor productivity.

Take, for example, the Thousand Talents Plan, which is now in its 10th year of helping China to attract foreign researchers and to incentive Chinese scientists living abroad to return home (Jia 2018). In 2008, China's central government declared the Thousand Talents Plan a scheme to entice leading Chinese scientists, academics, and entrepreneurs living abroad back to China. In 2011, the scheme grew to incorporate younger talent and foreign scientists, and a decade later, Thousand Talents has attracted more than 7,000 people total (Jia 2018). For Chinese scientists, the scheme has provided them a powerful financial motivation to return home. For immigrants, it is an opening to join the Chinese rule with significant administrative difficulties eliminated. In the research community, scientists selected for talent projects gain access to much higher salaries and research funding levels than their locally qualified peers. Thousand Talents proves more formidable than other plans, aiming to target professors and chief scientists in the west.

Ten-Year Plans in connection to education.

The Chinese Communist Party's Central Committee is concerned with education as a means to sustain its control and power solidly over its people. Past failures of various definitions for "individualistic property rights" were promoted in China by the first Ten-Year Plan during the 1930s. The warlord Yen Hsi-shan attempted to modernize the weak Chinese economy in his province by carrying out the Ten-Year Plan of Economic Reconstruction (Gillin 1965). Yen's outline for promoting economic growth in Shansi, China's First Five-Year Plan, was inspired by the success of Stalin's first Five-Year Plan for the Soviet Union (Gillin 1965).

The growth of the Soviet Union during the Great Depression caused other countries that were previously anti-Communist to look to the Soviet Union for a solution to economic difficulties. During the 1930s, Yen and his followers frequently lavished admiration on the Soviet Union for its dramatic accomplishments in the field of industrial development and advocated adopting their methods of growth in order to achieve similar results in China. Yen believed that the Soviet Union industrialized more in one year than other countries advanced in five years. (Gillin 1965).

The first Ten-Year Plan attempted to reduce the autonomy commonly enjoyed by local officials in Shansi through economic controls created by the reinforced determination to concentrate authority in the hands of a Chinese warlord. Soviet successes caused Yen to become acutely conscious of the immense power possible if China's vast population were liberated together, not singularly. It not only caused him to overlook the economic interests of the rich, but also demonstrates why he tried to educate the masses and urged them to engage more actively in economic affairs. Yen's determination to build an industrialized power-state exceeded both his ambition for the state's participation and his anxiety of a social or economic revolution.

Higher-learning institutes in China built by Russian immigrants.

During the first half of the 20th century, Russian emigrants in China established a system of higher learning based on prerevolutionary Russian educational systems. These institutions played a role in strengthening the Chinese intelligentsia, with Russian faculty successfully training future engineers, lawyers, Orientalist scholars, teachers, theologians, and musicians (Khisamutdinov 2016). Today's higher-education reforms in China are without this generation, considering the knowledge of Russian emigrants in China, detailed in the following paragraphs.

During the Russian Civil War (1918 to 1922), hundreds of thousands of Russian refugees lived in China. These Russian emigrants tried to settle close to the border because they assumed to return to their country as soon as the communists fell from power (Khisamutdinov 2016). In the beginning period of the emigration, most emigrants stayed in Harbin, which was built by Russians as an administrative, educational hub center for the Chinese Eastern Railway (CER). Harbin had Russian schools, Russians made up a substantial part of the population, and the administration, police, court, and other institutions functioned under Russian laws until 1924.

Once they graduated from local schools, the children of the initial builders and railway employees could advance their education only in their homeland, although the matter of higher-education institutions for the CER zone had already been raised in 1916 when the Committee for Higher Education formed at the enterprise of the railway administration. The most significant historical and educational value of China's establishments also played a role in developing the Chinese thought leaders, with Russian talent famously training future engineers, lawyers, Orientalist scholars, teachers, theologians, and musicians. The political issues in China pushed many Russians emigrants to new sanctuaries to successfully continue their academic careers (Khisamutdinov 2016).

Iran.

The 2019 Worldwide Threat Assessment of the US Intelligence Community has deemed Iran as a presence in cyber espionage and attacks. Iran uses increasingly advanced cyber systems to direct espionage. Additionally, the nation also is attempting to deploy cyber attacks that would facilitate crimes against critical infrastructure in the US and its allied countries. Through the use of social media platforms to target these associated audiences, Iranians are targeting American government officials, government organizations, and corporations to gain intelligence and position themselves for impending cyber operations. Iran has been developing cyber attacks against the US and its allies for some time (Coats 2019).

These actors are skilled in causing localized, temporary effects such as disrupting a large company's corporate network for days to weeks, comparable to its data deletion attacks against dozens of Saudi governmental and private-sector systems in late 2016 and early 2017. This behavior is not new from the Iranians; an indictment filed by a federal grand jury in New York City (unsealed in 2018) claimed that Iranian hackers stole 31.5 terabytes of data, including scientific research, journal articles, and dissertations (Cohen 2018). The victims included 7,998 professors at 320 universities around the world over the past five years.

In what the Department of Justice has reported as one of the most massive state-sponsored hacking attacks (APT), nine Iranians acting on the support of the Islamic Revolutionary Guard Corps carried out this large-scale mission (Cohen 2018). Host institutions paid more than $3.4 billion to procure and access documents from an institute in Iran named Mabna that allegedly was set up by the accused and that coordinated and paid for the hacks. The members of the plot employed stolen account credentials to gain unapproved admittance to victim professors' accounts, which they utilized to steal research and other academic data and documents, including, among other things, academic journal articles, theses, dissertations, and electronic books (Nine Iranians Charged with Massive Cyber Theft 2018). The defendants targeted data across all fields of research and academic disciplines, including science and technology, engineering, social sciences, medicine, and other professional fields. The charges against the indicated comprise wire fraud, aggravated identity theft, and conspiracy to commit computer intrusion.

The indictment stated the university breach as one of spearfishing, in which the accused sent emails to victims that deceived them into providing their login credentials (CohenMar 2018). The emails claimed to originate from individuals who had viewed articles written by the targeted professors; they claimed to be asking to see more of their academic work and rendered a link. A click on the link guided the victim to a fraudulent Internet domain that reflected their own university's website and prompted them to log in.

Since these acts, American intelligence agencies have singled out Iran as one of the leading foreign cyber threats facing America, along with Russia and China. As a result, The Trump administration has reimposed sanctions on Iran to prevent its aggression, denying the country funds it needs to finance terrorism and its missile program (Riechmann 2019).

Naïveté about the threat of foreign espionage.

The number of international students and researchers in America has grown dramatically in recent decades, and with the globalization of American universities, the frontlines of education now serve as both foreign and domestic espionage hubs. International and domestic intelligence agencies actively are choosing sources and informants on American college campuses (Award-Winning Journalist Discusses Presence of Spies on Campuses 2018). Foreign and domestic intelligence agencies actively are recruiting subjects and experts on American college campuses.

Take, for example, the Central Intelligence Agency (CIA), which has tried and failed to recruit foreign nuclear scientists as spies because foreign nationals choose instead to hold temporary positions at universities such as Princeton (Award-Winning Journalist Discusses Presence of Spies on Campuses 2018). Another government agent befriended a scientist and regularly asked him to contribute more and more information about his work. Finally, the scientist asked to talk with the FBI on the condition that it would help his son gain acceptance into an American college.

Even further, an academic individual with the moniker Cynthia Murphy ingratiated herself as a critical fundraiser for Hillary Clinton’s 2008 presidential campaign. She was to report findings to Moscow after establishing daily ties with classmates and professors who could help with job searching and who held secret information and detailed personal data and character traits; findings were to include preparatory judgments about the potential vulnerability of the classmates and professors to be recruited by the Russians.

How Intellectual Property Theft Has Been Addressed in the Past

The issue of protecting IP from foreign entities is not new. Protecting research has been a concern for many decades. This section discusses how this challenge has evolved over time.

World War II

The concern over security and classification prior to World War II was primarily the responsibility of the Department of War and the Armed Forces. Classified programs included the protection of military secrets and diplomatic communications (National Academy of Sciences 1982). During World War II, the responsibility for military research fell under the Office of Scientific Research and Development (OSRD). The OSRD used the same classification system as the Armed Forces, but it had to keep information at the lowest classification possible to communicate and interact with the university environment.

When the wars ended in Europe and the Pacific, the OSRD was faced with the problem of declassifying scientific and industrial information that had been achieved or collected during the war. Some information was released to the public, but most of the scientific research was placed under security restrictions. The Massachusetts Institute of Technology (MIT) Radiation Laboratory was the primary microwave radar research facility in the US after the war. This facility is a great example of the benefits provided to universities and industry from R&D conducted during the 1940s (National Academy of Sciences 1982).

Atomic energy era.

The postwar period saw the rise of the US and the Soviet Union as the two global superpowers. As a result, the federal government became increasingly concerned about the protection of scientific information. One of the first major legislations aimed at protecting this information was the Atomic Energy Act of 1946. This act restricted the release of information about the Manhattan Project, and in 1954 the act was amended to make all atomic energy information secret at the time of its creation (National Academy of Sciences 1982).

Export control.

World War II also created the framework for US export control systems. The end of the war saw the creation of the Export Control Act of 1949. This act was designed to screen exports to the Soviet Union and other communist countries under the Iron Curtain. The 1949 document was followed by the Export Administration Act of 1969 and the Export Administration Act of 1979. These acts were passed with the intention of preventing exportation of goods that could assist the economic or military potential of communist countries (National Academy of Sciences 1982). The International Traffic in Arms Regulations were established as part of the Mutual Security Act of 1954. The rules set forth were to control the export of military systems, including plans, designs, and production techniques of items on the Military Munitions List or any item that could have military applications.

Committee and office creation.

The Coordinating Committee for National Export Controls (CoCom) was established in 1949 with the intent of organizing North Atlantic Treaty Organization (NATO) allies plus Japan around trade policies with the People's Republic of China and the Warsaw Pact countries. Established within the Department of Commerce by the Eisenhower Administration in 1954, the Office of Strategic Information (OSI) was another measure to stem the flow of industrial and military information being transferred to the Soviet Union. Congress decided to terminate the OSI in 1957 because of the negative impact had on scientific projects (National Academy of Sciences 1982).

Restrictions on foreign entrants.

Restricting foreign nationals entering the US is another postwar method that has been used to prevent the transfer of information, in addition to classification and export controls. The Internal Security Act of 1950 and the Immigration and Naturalization Act of 1952 made it much more difficult for scientists without US citizenship to receive grants or find work within the US. It was also during this timeframe that the US Congress became concerned with the loyalty of scientists conducting unclassified research with the aid of federal grants (National Academy of Sciences 1982). The case of Dr. N.V. Umnov in 1980 is an example of a Soviet scientist only being permitted to study his specialty, robotics, at a theoretical level. Dr. Umnov was not allowed to visit industrial facilities in the US, and he was denied access to production research and any classified or unclassified research programs funded by the Department of Defense because of his nationality (National Academy of Sciences 1982).

Patent review.

The Patent and Invention Secrecy Act of 1951 required sending to the Department of Defense for review all requests for patents with possible military applications. President Eisenhower updated the rules for classification with the release of Executive Order 10501, Safeguarding Official Information in the Interests of the Defense of the United States, in November 1953 (Eisenhower 1953). Generally speaking, the rules were relaxed compared to the Truman-era version of this document.

Sputnik I and Dual-Use Technologies

The 1957 launch of Sputnik I shifted the perception of the technology race between the US and the Soviet Union. The Kennedy Administration recognized that the US was falling behind and took steps to rebuild America's competitive edge. The Export Administration Act of 1969 signaled a shift in thawing trade relations between the two countries. The act openly encouraged trade with all nations, including communist countries, in hopes that the state of international affairs would remain calm (National Academy of Sciences 1982).

By the mid-1970s, it was becoming apparent that it was much more challenging to separate military applications from civilian technologies. Facing these new challenges, the Defense Science Board commissioned a task force on export control of US technology. The task force found design and manufacturing know-how to be the principal elements of strategic technology controls, in addition to any product with direct military applications (Office of the Director Defense Research and Engineering 1976).

Shortly after this task force released its findings, the Arms Control Act of 1976 and the Nuclear Nonproliferation Act of 1978 came into effect. Both acts imposed restrictions on the movement of products and plans related to militarily critical technologies outside of the US (National Academy of Sciences 1982). Significantly, the Export Administration Act of 1979 focused specifically on the export of technologies rather than just goods. The recommendations of the 1976 Defense Science Board task force were being put into effect. One of the provisions of the Export Administration Act of 1979 was the creation of the Military Critical Technologies List (MCTL). The list identifies technological elements essential to advanced military capability, emphasizing manufacturing know-how, equipment, goods, and maintenance know-how (National Academy of Sciences 1982).

Early 1980s—Wake-Up Call

The early 1980s was a period in America where the threat from Soviet intelligence services on the academic community started to gain traction in Washington, DC. The release of the 1981 Soviet Military Power report was a wake-up call for the US, particularly for the science and technology communities. The Soviets were closing the gap in a number of technology areas including electro-optical sensors, guidance and navigation, hydroacoustics, and optics and propulsion (Department of Defense 1981). Soviet military advances in submarine forces and weapons were a direct representation of the investment in science and technology. At the time of the 1981 Soviet Military Power report, the Soviet Union was believed to have 900,000 full-time scientists and engineers engaged in R&D compared to only 600,000 in the US (Department of Defense 1981). In 1980, the Soviet Union graduated 300,000 engineers from a total pool of 800,000 students (Department of Defense 1981). The report also cited that in 1965 the US had maintained a 10- to 12-year development and production gap ahead of the Soviets in microelectronics and computers. By 1980, that gap had been closed to two years, mainly attributable to the copying and reverse engineering of US technologies (Department of Defense 1981). Looking at Soviet microprocessors, it became very apparent that they were engineered from US integrated circuits.

Most of the life sciences research conducted during this timeframe centered around improving the human within the weapons system. The Soviets invested in underwater physiology, submarine habitability, and aviation physiology to improve their military competitive edge (Department of Defense

1981). All unclassified research reports conducted by the US government were forwarded to National Technical Information Services (NTIS) under the Department of Commerce and were made available publicly for a very small fee. Until the Soviets' permissions were revoked in 1980, they had purchased 80,000 documents from the NTIS database each year (Department of Defense 1981). This basic research saved the Soviets time and money in the R&D phases of weapons production. Any research efforts that dead-ended for the US were avoided by the Soviets, and as a result, the technological advantage maintained by the US began to decrease. Research in biological weapons was not a major threat during this time period, but the Soviets continued to invest in biological R&D activities.

From 1970 to 1980, the Soviet Union had launched 75 spacecraft per year, a rate 5 times more that of the US (Department of Defense 1981). The annual payload in space amounted to 10 times more than the US at 660,000 pounds (Department of Defense 1981).

Academic exchanges.

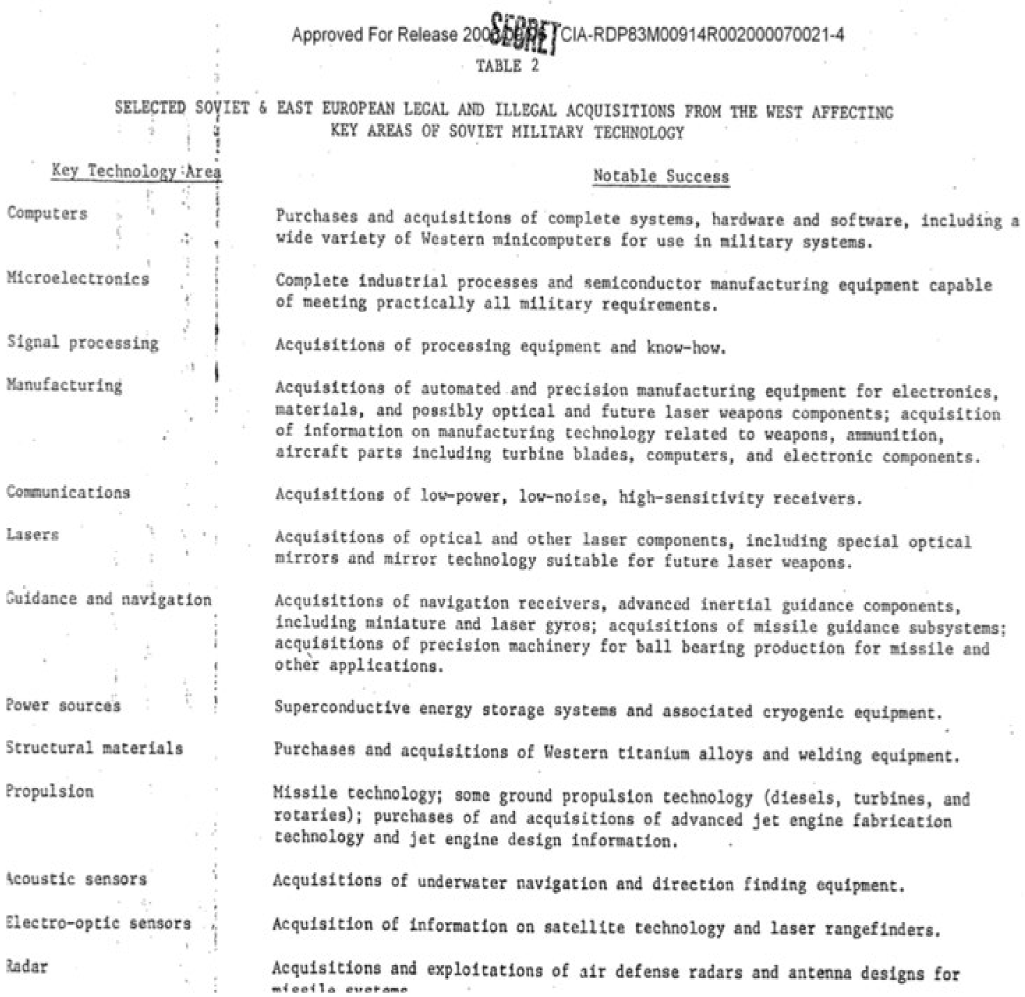
During this period, the US and Soviet governments did authorize science and technology exchanges. There were exchanges of scientists and technical information, documentation, joint research, and research results (Department of Defense 1981). Inter-Academy exchanges were common, as well as PhD candidates from both countries. Conferences and symposiums were used to advertise research to private companies to secure contracts; these served as another avenue that the Soviets would exploit for technology exchange.

Soviet acquisitions report.

In 1982, the CIA released a report of how the US's technical advantage had eroded and what the security implications were. The report cited that the overwhelming share of "military significant" technology and equipment was acquired through clandestine acquisition and illegal trade (U.S. Central Intelligence Agency 1982). Soviet intelligence services also placed a high priority on acquiring fundamental research that correlated directly with genetic engineering and laser technologies. In a targeting effort of western universities, professors actively were recruited to teach in Warsaw Pact schools that had a specific skillset with military applications. The Soviets were pursuing technologies before military applications could be identified and before US security controls were implemented (U.S. Central Intelligence Agency 1982). These collection activities normally were conducted at technology trade shows and visits to commercial firms in the US.

In 1981, a Hughes aircraft engineer was arrested and charged with selling US secret documents to an eastern European intelligence officer employed by a Polish-owned, US-chartered Illinois firm (U.S. Central Intelligence Agency 1982). Figure 2 shows a comprehensive list of illegal acquisitions from the west affecting key areas of Soviet military technology (U.S. Central Intelligence

Agency 1982, 16).



Approved For Release 200[illegible] SECRET CIA-RDP83M00914R002000070021-4

TABLE 2

SELECTED SOVIET & EAST EUROPEAN LEGAL AND ILLEGAL ACQUISITIONS FROM THE WEST AFFECTING KEY AREAS OF SOVIET MILITARY TECHNOLOGY

Key Technology Area	Notable Success
Computers	Purchases and acquisitions of complete systems, hardware and software, including a wide variety of Western minicomputers for use in military systems.
Microelectronics	Complete industrial processes and semiconductor manufacturing equipment capable of meeting practically all military requirements.
Signal processing	Acquisitions of processing equipment and know-how.
Manufacturing	Acquisitions of automated and precision manufacturing equipment for electronics, materials, and possibly optical and future laser weapons components; acquisition of information on manufacturing technology related to weapons, ammunition, aircraft parts including turbine blades, computers, and electronic components.
Communications	Acquisitions of low-power, low-noise, high-sensitivity receivers.
Lasers	Acquisitions of optical and other laser components, including special optical mirrors and mirror technology suitable for future laser weapons.
Guidance and navigation	Acquisitions of navigation receivers, advanced inertial guidance components, including miniature and laser gyros; acquisitions of missile guidance subsystems; acquisitions of precision machinery for ball bearing production for missile and other applications.
Power sources	Superconductive energy storage systems and associated cryogenic equipment.
Structural materials	Purchases and acquisitions of Western titanium alloys and welding equipment.
Propulsion	Missile technology; some ground propulsion technology (diesels, turbines, and rotaries); purchases of and acquisitions of advanced jet engine fabrication technology and jet engine design information.
Acoustic sensors	Acquisitions of underwater navigation and direction finding equipment.
Electro-optic sensors	Acquisition of information on satellite technology and laser rangefinders.
Radar	Acquisitions and exploitations of air defense radars and antenna designs for missile systems

Figure 2. Acquisitions from the west affecting Soviet military technology.

Some of the key acquisitions on this list include missile guidance and control technologies. The Soviets used agents in US subsidiaries overseas to steal technical data manuals. One of the most famous industrial espionage cases was the acquisition of detailed specifications, plans, and technical drawings of the US Air Force C-5 Galaxy strategic airlift aircraft early in its development cycle (U.S. Central Intelligence Agency 1982). These technology gains by the Soviet Union saved hundreds of millions of dollars in R&D costs and years of development lead time. The Soviets were able to capitalize on proven western designs and minimize military production costs.

The Soviet Union was able to achieve greater weapons performance than if it had relied solely on its own technology, as assessed by the CIA (U.S. Central Intelligence Agency 1982). The 1982 report stated that while the direct impact of east-west trade on Soviet military power could not be quantified, it was clear that western military production would have to compete against capabilities derived from western technologies and that the benefits of legal sales to the Soviets were not considered to outweigh the costs of those exchanges (U.S. Central Intelligence Agency 1982). The report warned that US universities and sensitive-but-unclassified US technical data would be targeted in the coming years and that the scientific communities were not prepared or aware enough to deal with this threat. The Soviets were expected to shift their intelligence efforts toward the commercial and academic sectors during the 1980s, resulting in a security shift to begin addressing security threats in the academic environment.

The findings of this intelligence report clearly stated that although the Soviets used the US's openness to their military advantage, the US prized too highly that openness and the resultant academic and industrial benefits to close it off unthinkably (U.S. Central Intelligence Agency 1982). The CIA report supported open academic exchange; however, the science and national security communities were urged to take steps to identify and protect new and emerging technologies with critical industrial or future weapons applications.

Scientific communication and national security panel, 1982.

In March 1982, officials from the academic community and the Department of Defense hosted a panel on scientific communication and national security to address the growing concern of protecting research from foreign adversaries, specifically the Soviet Union, without damaging scientific progress and its contribution to the national welfare. It was determined that the Soviet Union was exploiting its exchange programs with the US by giving intelligence collection assignments to some of its participating nationals (National Academy of Sciences 1982). Some of the exchange scholars from Soviet countries were conducting research beyond their agreed-upon fields of study. The overarching consensus from this panel was that the benefits of free exchange of science and technology do not outweigh the costs of closing or restricting the academic environment:

> There is a strong consensus, however, that universities and open scientific communication have been the source of very little of this technology transfer problem. Although there is a net flow of

> scientific information from the United States to the Soviet Union, consistent with the generally more advanced status of U.S. science, there is serious doubt as to whether the Soviets can reap significant direct military benefits from this flow in the near term. (National Academy of Sciences 1982)

Classification, export controls, funding, and foreign nationals.

The panel recognized the existence of a number of control systems in place to deal with the communication of scientific information. The first classification is that used to control sensitive information with national security implications. The second is export control measures to protect information from foreign nationals, such as the Export Administration Act and its associated Export Administration Regulations and the Arms Export Control Act and its associated International Traffic in Arms Regulations (National Academy of Sciences 1982). The third method of control comes from research funding sources. Projects funded by organizations such as the Department of Defense may be emplaced with restrictions on publication. The Department of Defense may require prepublication review of research topics believed to have national security implications. Voluntary agreements with researchers can limit the flow of technical information or negotiate alterations before publication. The final method is foreign nationals being denied entrance into the US to protect scientific information. The government could deny visa requests or mandate restrictions on individuals once they have entered the country (National Academy of Sciences 1982). Under specific scientific exchange programs, Soviet or eastern European visitors could be limited admission into the US.

Openness, classification, and gray area.

When looking at the categories of university research, three different types of information were identified by the panel. The first category of research identified was research for which openness overshadows any possible near-term military benefits to the Soviet Union (National Academy of Sciences 1982). The second category identified was research for which classification is clearly the right choice under the auspice of national security. In these circumstances, government-supported research resulting in military applications in a short time should consider classification. The third category, known as the gray area, was identified as research that does not require classification but requires limited restrictions to protect it.

The panel recommended that for basic or applied research to become controlled in any way, it must meet all four of the following criteria:

1. The technology is developing rapidly, and the time from basic science to application is short;
2. The technology has identifiable direct military applications; or it is dual-use and involves process or production-related techniques;

3. Transfer of the technology would give the U.S.S.R. a significant near-term military benefit; and
4. The U.S. is the only source of information about the technology, or other friendly nations that could also be the source have control systems as secure as ours. (National Academy of Sciences 1982, 5)

It was determined that if the above criteria were met but classification was still not appropriate, there were measures that could be put in place to preserve the openness of science while still meeting the security needs of the government.

The first measure was restricting foreign nationals from working on the project but not limiting their access to university spaces or enrollment in classes. The second measure stipulated that research publications be submitted simultaneously to the publisher and the Department of Defense or federal agency contracting officer. The government would be allowed 60 days to recommend changes to the manuscripts (National Academy of Sciences 1982). This information was still considered unclassified research; therefore, the university still had the right to publish, but the federal government could seek the option to classify as appropriate in accordance with federal regulations.

Export Administration Regulations and International Traffic in Arms Regulations should be used between science and industry for unclassified information that does not have any national security implications. A general license grants exemption from the formal licensing process. The MCTL has been recognized as an important tool that can be used in the limited technology and research areas where controls have been deemed appropriate (National Academy of Sciences 1982). This list requires updating to reflect accurately some of the more rapid innovations being made today. At the time of the panel, the US was transferring industrial technologies to the People's Republic of China as part of a program to help advance "third world countries." There were concerns that technologies could be transferred to the military sector and that these countries could potentially become adversaries in the future.

Task force on university responsiveness, 1982.

With additional restrictions being imposed on America's colleges and universities, the Defense Science Board launched another task force. The 1982 Task Force on University Responsiveness was meant to find out if universities were interested in and able to support national security requirements in both manpower training and basic research (Department of Defense 1982). The task force also investigated what role the Department of Defense should play with the NSF in support of basic research, as well as the problems caused by the high percentage of foreign nationals in science and engineering fields (Department of Defense 1982).

The director of the Very High Speed Integrated Circuit (VHSIC) program released a memorandum on December 12, 1980 that attempted to restrict publication of unclassified university research results in connection with

Department of Defense–sponsored research projects and to restrict foreign scholars from participating in these projects (National Academy of Sciences 1982). Multiple US universities protested the memo, requiring creation of the Defense Science Board Task Force on VHSIC. The task force came up with the following recommendations: "(1) no controls on basic research, (2) research with commercial proprietary value should be subject to EAR, (3) dual-use research that has distinct military sensitivity should be regulated under ITAR, and (4) single-use defense technology should be classified projects (National Academy of Sciences 1982, 105).

The Millennium

Task force on basic research, 2012.

In 2012, the Defense Science Board released the Report of the Defense Science Board Task Force on Basic Research. It identified a number of impediments preventing the Department of Defense's research program from functioning as smoothly as possible. The board also recommended doubling the existing doctoral fellowship programs within the National Defense Education Program (Defense Science Board 2012). To make these fellowship programs more competitive, stipends needed to be provided to compete more closely with other civilian research programs. Another major finding of the Defense Science Board was the globalization of basic research and the importance of working side-by-side with foreign scientists. The task force recommended increasing foreign basic research from 3% to 5% and increasing invitations to foreign scientists (Defense Science Board 2012).

National Security Higher Education Advisory Board disestablishment.

In February 2018, the unit chief of the FBI Office of the Private Sector dispatched a letter to the National Security Higher Education Advisory Board (NSHEAB) announcing its disestablishment. The NSHEAB was a forum for discussion of national security issues between leaders of the higher-education community and federal agencies, including the FBI, CIA, National Security Agency, Office of National Intelligence, and Department of Defense (Mitchell 2018).

The letter from the FBI stated that because of restructuring, the academic community would have to engage the FBI through other means, but that communication with academia would remain a priority for the FBI (Federal Bureau of Investigation 2018). The president of the American Council on Education (ACE) responded to the FBI director to express concern over the disestablishment of the NSHEAB. The ACE recognized the recent heightened security concerns regarding international students and purported to be looking for a way to rebuild the relationship that the NSHEAB created between academia and government agencies (Mitchell 2018).

Policy Affecting Intellectual Property Theft

As information theft has existed for several decades, there are plenty of policies affecting the issue. This section summarizes some of the major policies that affect this problem. Understanding historical policy provides insight into how the issue has evolved over time, which can inform future recommendations to address the current state of the problem.

National Security Decision Directive 189.

In 1985, the Reagan Administration released national-level policy on controlling the flow of science and technology in federally funded fundamental research labs. National Security Decision Directive (NSDD) 189 provided a comprehensive definition of what qualifies as fundamental research, and it would be the policy of the administration to ensure that products of fundamental research were kept unrestricted to the maximum extent possible (The White House 1985). This policy was based on the 1982 Scientific Communication and National Security report, which determined that significant technology was being transferred to the Soviet Union but that open scientific communication of fundamental research was only a minor contributor to the overall problem (The White House 1985).

In November 2001, Condoleezza Rice, Assistant to the President for National Security Affairs, briefed the Council on the Future of Technology and Public Policy regarding export controls and fundamental research. She stated that the current administration would continue to support the provisions of NSDD 189. The free exchange of ideas and science would continue to be key to US national security (Rice 2001).

In 2008, John Young, Under Secretary of Defense for Acquisition Technology and Logistics, released a memorandum to the secretaries of the military departments and joint staff to reinforce the language of NSDD 189. The memorandum also clarified the definitions of fundamental research and contracted fundamental research. It would be the policy of the Department of Defense not to restrict disclosure of the results of contracted fundamental research unless the research were classified for reasons of national security (Young 2008). Again in 2010, Ash Carter, Under Secretary of Defense for Acquisition Technology and Logistics, released a memorandum on the importance of keeping fundamental research free and open. Products of fundamental research were to remain unrestricted to the maximum extent possible, and classification was viewed as the only appropriate mechanism for restricting this information (Carter 2010). These memorandums and NSDD 189 continue to remain the policy documents governing the Department of Defense Basic Research Office.

Department of Defense policy.

Department of Defense Instruction 3210.1 lays out the department's priorities and conduct for support of basic research. It explains the importance of basic research and its position as a long-term investment in the nation's future

(Department of Defense 2018). This instruction follows the principles outlined in President Clinton's 2000 Executive Order 13185, which was designed to strengthen the partnership of the government and university research. The executive order created four key provisions for the government and universities: research is an investment in the future; the integration of research and education is vital; excellence is promoted when investments are guided by merit review; and research must be conducted with integrity (Clinton 2000).

National security and defense strategies.

It is important to note how the current administration views the threat posed by Russia and China to national security. The 2017 National Security Strategy acknowledged China and Russia as seeking to challenge American power, influence, and interests and attempting to erode American security and prosperity (Trump 2017). The document stated that the US must preserve its lead in research and technology and protect the economy from competitors who unfairly acquire IP (Trump 2017). Departments and agencies must eliminate unnecessary regulations that stifle growth, drive up costs, and impede R&D (Trump 2017). The US must continue to attract the innovative and the inventive and must invest in early-stage R&D (Trump 2017). These strategy points reinforce the importance of free exchange and recruiting talent.

The National Defense Strategy released by the Pentagon followed the lead of the National Security Strategy, but it pointed to a strategic shift in the balance of power. Interstate strategic competition, not terrorism, was noted as the primary concern in US national security (Mattis 2018). The Department of Defense has shifted to meet this new enemy, and the US military and R&D competitive advantage are concerns. Shortly after the release of the National Defense Strategy, Secretary Mattis released a memorandum establishing the Protecting Critical Technology Task Force. The urgency of this task force was cited because American industry loses more than $600 billion dollars to theft and expropriation each year (Mattis 2018). The document also cited concern for the loss of classified and controlled unclassified information. The academic community must recognize this shift as it did in the 1980s—that American universities are a soft target and that Russia and China seek to capitalize on free and open exchange provided by the US.

Reframing the Issue

The dialogue surrounding the issue of IP theft by foreign individuals is complex. A significant factor adding to the complexity is the fact that both sides of the problem solvers seem to be talking *at* each other rather than *to* each other. One side takes the viewpoint that foreign research assistance from particular countries could be bad actors, and the other side asserts that research is a pivotal part of human advancement and must not be hindered by petty issues.

During the research conducted by this team, it became clear that two key concepts need to be clarified so that proper dialogue can occur to effectively address the problem: (1) IP theft versus intellectual capital loss and (2) understanding the real issue behind the concerns of foreign research assistance—general security for research projects. Once these items are defined and framed, the research team believes that clear communication can occur to work on the problem and address it properly.

Intellectual Property Theft Versus Intellectual Capital Loss

IP theft implies that information was identified explicitly as valuable and then was stolen. One challenge inherent in this discussion is that, often, no one knows if the product of research will be significant until after the research is conducted or is at least near complete. And so while processes do exist to protect sensitive or significant research, the research must be classified as such from the beginning to prevent malicious parties from being involved—a classic Catch-22.

With an increasingly global and technology-based economy, it has become very difficult to understand the implications of each new discovery. Assuming that every piece of research will become sensitive or valuable would create restrictive controls that hinder the advancement of science and information sharing. Failing to address the concern that research will become sensitive or classified invites the opportunity for bad actors to steal a valuable product.

Hence, the real concern is the loss of intellectual capital. Intellectual capital implies that there could be valuable content created during research that later would become IP. Understanding this distinction creates a framework and vocabulary with which to address the issue—it does not change the primary issue of not knowing whether a research effort will be valuable, although sometimes it is known whether research will be sensitive or classified. Thus, this team suggests that the real issue is not IP theft, but intellectual capital loss, which can be in the form of IP theft. Framing the problem in this way creates the need to address protecting research and its eventual product proactively and allows both sides to explore the issue properly.

Foreign Researcher Issue Versus General Security Issue

The government has strong concerns about using foreign researchers on government-funded research projects (Department of Defense 2018, Edwards 2016, Gamache, Senator Cornyn questions for the record for Dr. Kevin Gamache, Chief Security Officer, Texas A&M University System 2018). These concerns stem from the fact that other countries have a vested interest in developing intellectual capital and IP to advance their agendas. Many nations are working to develop capital and IP to foster economic growth and other capabilities.

While these concerns are not unfounded, the real issue is securing research projects properly and ensuring that information is not obtained by those who are not authorized to have it. As such, this needs to be seen as a general security problem or an information security problem. Research teams in the universities that house them need to have proper security in place to protect research. The truth of the matter is that no one wants *anyone* to take information wrongfully and distribute it or use it without proper permission—whether it's being taken by a foreign researcher or an American research student with malicious intent.

Consequently, the narrative needs to evolve to focus on having proper security practices in place to protect valuable research so that it can be released at the appropriate time to the appropriate parties. By changing the narrative and focusing on the fundamental issue, both sides can discuss the problem in a meaningful way and ensure that research is safe, not only from the perceived bad actors today, but from any bad actors in the future. The variables affecting this problem are far more than nation-states sending students to American universities to become researchers.

As previously discussed, there is a shortage of researchers in the US, and talent is scarce. Further, the convenience and collaboration offered by the Internet makes it much easier for bad actors to attempt to gain access to valuable material. It's unfortunate, but the same technology that makes it possible to share information instantly also makes it possible to steal information just as quickly. Consequently, all of the issues that affect this problem must be taken into account when examining it.

Recommendations to Address Theft and Preserve Academic Freedom

This section provides recommendations from the research team on how government concerns around IP theft and intellectual capital loss might be addressed. These recommendations are based upon an examination of the literature review, research team analysis, discussions with AAU and APLU contacts, and an AAU and APLU member-institution survey on best practices (AAU & APLU 2019).

As the discussion in this report indicates, fundamental research is a vital part of economic growth and new scientific discovery. For this reason, properly protecting the product of research is essential. The following list of recommendations is offered as a means to address the problem of intellectual capital loss while simultaneously preserving the practice of fundamental research. These recommendations are divided into two categories, those made by the research team based on general research and those based on the best practices shared from the AAU and APLU member-institution survey. Research team recommendations are annotated by the acronym RT, and survey-based recommendations are annotated by the acronym SR.

Core Principles

Two core principles were observed in making recommendations to address the problem. The first is protecting the concept of fundamental research and the free flow of information. As previously discussed, fundamental research has made countless scientific advances that are critical to human existence and have benefited the entire world for generations, from aviation to medicine to forensics to meteorology to astronomy to digitization—the list goes on and on.

The second core principle is preserving the free flow of research talent. As there is a critical shortage of research talent, finding research assistance can be challenging, particularly in high-need areas such as technology, where undergraduate students can enter the workforce and earn six-figure salaries (Metz 2018, Sample 2017). With research talent being in such low supply, preference was given by the team to recommendations that offer preservation of the ability to acquire talent where available.

Research Team Recommendations

The following recommendations were developed by the research team after reviewing the available literature and applying the risk management framework. The research team explored information from a broad range of data sources and then worked together to formulate recommendations based on internal collaboration and discussions with members of the AAU and APLU.

RT1: Implement research communication agreements.

One of the government's strongest concerns regarding research, especially research funded by the federal government, is the possibility of intellectual capital loss or property theft by untrustworthy or bad-acting members of the research team (insider threats). Essentially, the fear is that a member of the team will release or sell the information before it is properly protected or distributed as intended. One way to address this concern is to implement research communication agreements for all members of a research team.

A research communication agreement outlines the communication protocol for a research team. It holds members responsible for ethical obligations to keep research materials confidential and appropriately protects and outlines the appropriate messaging for releasing and sharing research-related data. This practice sets expectations and ensures that information is not released when it should not be, either accidentally or intentionally.

Moreover, establishing a baseline for communication protocol helps address the government's concern about information being leaked intentionally from bad actors inside the research team. Not only does this baseline address the concern voiced by the government, it is also a standard practice used by the government and countless organizations in the private sector. Also, this solution reinforces the sensitivity of the research to the research team to help them internalize information security better.

Lastly, one of the more complex issues regarding government research is the desire to protect potentially sensitive research results. This issue traditionally has acted as a Catch-22 because research must be regarded upfront as classified based on value, but it's difficult to know if the results of research will be sensitive or valuable until after the research is conducted and the results are produced. A communication agreement represents a middle ground, providing a layer of security while the research is occurring so that the principal investigator can determine if the research is sensitive and engage the proper process to protect the research.

While it’s easy to suggest that the responsibility for understanding when research becomes sensitive belongs to the government program manager, all stakeholders should have a vested interest in protecting valuable information and ensuring that it’s handled appropriately. Working under a communication agreement enables all stakeholders to be more effective in protecting information.

RT2: Create a scholarship incentive program—National Science Scholarship for Service.

Scholarship incentive programs have worked well to develop new talent when needed. Typically, these programs are referred to as *scholarship for service*. One such example is the CyberCorps®: Scholarship for Service funded by the NSF (OPM 2019). This program provides up to two years of tuition, as well as a living stipend, to third- and fourth-year undergraduate and graduate students. In exchange for these benefits, students agree to give a year of service for each year paid for by the program. Students can fulfill their service obligation by working for government agencies at the federal, state, local, or tribal level. If students do not fulfill their service obligation, they agree to repay the funds expended on their behalf as a loan.

These programs have been in place for more than two decades and have a strong history of producing new talent. The research team recommends that a program be created to facilitate increasing research talent in the US with the suggested name National Science Scholarship for Service. We suggest that this program be modeled after other scholarship-for-service programs, where awardees receive full tuition and a living stipend and be asked to work in a research-based job for two years for each year paid for by the government.

RT3: Recruit more research talent from undergraduate and graduate students.

The only way to get more research talent inside the US is to create more research talent from within. Universities should work within their own student base to develop future researchers and encourage students to explore research opportunities. While this has always been a goal of research institutions, the dearth of research staff makes this a new imperative. Developing programs to garner interest in research and teach research skills should receive more resources and emphasis.

RT4: Create a path to citizenship for foreign researchers.

Another way to address the dearth of researchers available in the US and the strong need for research talent is to create a path to citizenship for foreign researchers. After attracting this talent and working with them to gain research skills, it makes sense to create an opportunity for them to stay in the US, perform important work, and add to the diversity of the population.

For example, a special student visa program could be created for research students who come to the US. After completing their degree programs, they could become eligible for a special work visa for researchers, similar to the H1B program for workers with in-demand skills. Upon obtaining this work visa, researchers would work for a four-year period, after which they would become eligible to obtain residency. They then could become American citizens in the normal course of the citizenship process.

This recommendation would go a long way in attracting top research talent and retaining the talent currently refining their skills. It further addresses the concern over foreign research talent being loyal to their foreign entities. Giving a foreign student the prospect of earning American citizenship would go a long way to mitigating this concern and would act as a hedge against foreign influence.

RT5: Collaborate to create a security capability maturity model.

CMMs long have been used in the technology industry and the private sector to describe having mature operations that are effective and utilize repeatable processes. Research institutions should come together in a collaborative fashion and establish a university research security CMM. In this way, expert administrators and faculty could work together to define a model that would reflect the needs of academic research institutions uniquely.

With this model in place, institutions would work to obtain the appropriate level of capability. After an institution prepares itself, it then can submit for certification at the appropriate level. This process creates several value propositions. First, it would create a common nomenclature and vocabulary for understanding the preparedness status of an institution and what level of work it can process effectively and safely. Second, it would serve as an indicator by which to grant awarding institutions according to the level of maturity of the research institution's security model. Last, it would create a roadmap or template for individual institutions to improve their effectiveness.

Both the Department of Homeland Security and the National Institutes of Standards and Technology offer guidance on building and integrating CMMs (DHS 2014, NIST 2017). It is imperative that research institutions come together and work in a collaborative fashion to create a model that works explicitly for thems and their peer institutions. While this effort will take significant investment, the research team believes that these activities would create substantial value.

RT6: Implement noninvasive standardized secure research spaces.

Historically, one of the main challenges to security is that it often comes at the cost of convenience. This is a double-edged sword because if things are inconvenient they won't be used. And while convenient spaces are used more readily and frequently, information can be easily compromised. The team recommends that universities look at creating research spaces with preapproved secure infrastructure. Essentially, universities could look at creating pods for research work that would be preconfigured and would use known secure reference architecture for Internet connectivity, resource sharing, encryption, authentication schemes, and outside communication. The cyber security put in place in these pods should be as invisible as possible to the principal investigators and other researchers.

Creating secure and nonintrusive environments would ensure that research teams better embrace security protocols and can be protected. Further, because many of the security issues inherent in cyber security, such as encryption and secure access, would not inhibit research functions, it should be possible to create environments that are secure from cyber attacks but that do not inhibit research work. Working to derive a solution in this way would attack the problem at both ends, proactively ensuring that research areas are secure and that the users of the system, in this case researchers, fully participate and utilize best practices for security.

Recommendations Derived from Organizational Member Surveys

The following recommendations were derived from reviewing the best practices shared by AAU and APLU member institutions (AAU & APLU 2019). These ideas are particularly valuable because they come from groups working in the field daily to address the problem. Further, because the stakeholders who created these practices have a working knowledge of how academic institutions operate and what it takes to enact changes in policy, these recommendations are rooted in experience and practicality.

SR1: Implement information security awareness and mitigation strategies.

One of the results from the AAU and APLU survey of member institutions recommended a comprehensive communication campaign to increase the awareness of faculty and other campus community members of current reporting requirements (AAU & APLU 2019). The research team suggests that this recommendation be expanded to encompass a comprehensive communication campaign strategy regarding information security and research security.

Research has demonstrated that end-users are the most common vector for cyber threats (Aguilar 2015, Morgan 2017, Thomas 2018). Increasing user awareness through training has been shown to reduce security incidents and protect information. While many students and faculty are knowledgeable about technology, they may not realize the intricacies associated with this specific problem and that the university community members are specific targets. Several member institutions incorporate modules that discuss foreign entity–related security issues, such as protection of IP, export-controlled research, preserving scientific integrity, and specific guidelines for reporting suspicious behavior presented in faculty and student training on Responsible Conduct of Research (RCR).

SR2: Create high-level working groups and task forces.

Universities have a long-standing tradition of collaboration. Several AAU and APLU member institutions have created cross-campus working groups and task forces comprising senior faculty and administrators working together to deal with the issue of security threats from foreign entities (AAU & APLU 2019). This sort of collaboration is vital to sharing best practices and information, and the research team recommends that these working groups be expanded to more institutions. Further, these working groups could be used to execute the recommendations mentioned above, such as creating a CMM for research and other administrative procedures.

SR3: Develop guides and templates with which to review foreign contracts, grants, and gifts.

Establishing guides or templates for faculties and research teams to use provides hands-on guidance for relationships with foreign entities. Having these tools reinforces proper behavioral procedures. Further, this setup ensures that appropriate disclosure, reporting, and compliance with export control laws are used. Having written standards and templates or checklists is a time-tested and proven tool to ensure consistency, efficiency, and reliability for processes and critical tasks.

SR4: Establish a point of contact or liaison for federal security officials.

While it may be the responsibility of federal officials to provide oversight for government-funded research, it's in everyone's best interest to ensure that sensitive research products are identified early and cared for properly. Establishing a single point of accountability or contact for federal agencies would aid this effort greatly.

A single point of contact would help ensure that communication is concise and accurate. Additionally, having someone with a strong relationship with these agencies would enable institutions to keep up better with trends and changing guidelines, which would help with reacting quickly to new requirements and would limit surprises. Most importantly, it would cement a good working relationship among organizations.

SR5: Establish a foreign-affairs review office to complement the compliance control office.

Because interactions with foreign entities are under high scrutiny and can have ethical implications, universities should establish a foreign-affairs review office, which could be a similar body to an institutional review board. This organization could provide the previously recommended templates with which to review foreign contracts, grants, and gifts—templates that would help faculty and research teams manage their relations with foreign entities so they do not inadvertently engage in unwanted activity that would raise concerns with export control regulations. Additionally, this organization could provide a check-and-balance and review the template transactions. The organization could provide a rigorous review, ensuring that there are no export control violations and that proper disclosures are made.

The foreign-affairs review office also could create templates and guidelines for conflict-of-interest reporting requirements. Some institutions have implemented rigorous practices to identify faculty and researchers with foreign interests, as well as their affiliations with foreign institutions of higher education. The new office also could serve as an innovator in this area and work to identify new administrator policies and procedures, such as expanding conflict-of-interest policies to include conflict-of-commitment policies. Working proactively in this area would help ensure that there are no conflicts of interest with the institution that later could become problematic.

This office also could create a set of requirements for vetting foreign visitors. Many campuses hold policies that require faculty to notify university officials when foreign nationals are coming to visit and tour facilities. A recommended best practice is to have the hosting faculty member fill out a brief questionnaire or form for each visitor.

Many research universities have an export control compliance office, and those that do not should consider implementing one. These offices help facilitate the creation of export control policies and programs so that clear guidance exists in conducting research involved in export-controlled activities. This office also could provide outreach to faculty, administrators, staff, and students to create awareness about export control policies and to ensure appropriate implementation of technical control plans. Additionally, this office could review contracts and agreements with foreign entities and other sponsors of research, as well as grant terms, to ensure compliance with export control requirements. Placing these two offices in close proximity to each other, given their similar missions, could create synergy, information-sharing, and resource-sharing opportunities that would strengthen the ability of research institutions to address the issue of IP theft.

SR6: Create robust disclosure requirements for intellectual property.

Several institutions have identified the need to require specific disclosure of IP that has the potential for commercialization. Faculty are encouraged to identify IP with strong commercial value early so that efforts can be made to protect it, such as applying for patent protection. This practice helps ensure that IP is identified quickly and protected for future use and distribution.

SR7: Develop a process for travel and provide safeguards for traveling faculty.

Multiple research institutions have created programs to review faculty travel. Often these programs are administered by the export control compliance office. Activities conducted in this effort include reviewing software-use restrictions and other security and safety concerns. Specific actions included in this process are items such as cleaning and hardening devices including smart phones, tablets, laptops, and other electronic devices to ensure that they are safe from cyber attacks after travel to specific countries that are considered known threats.

Summary

The US government has identified intellectual capital loss and IP theft as a significant danger to research institutions. Consequently, there are many proposals being considered to address this problem that could have drastic ramifications for research institutions. These recommendations could result in the reduction of funding available for research projects, restrictions on the ability to use foreign research talent, new classification standards that inhibit the ability to conduct fundamental research, and the perception that foreign students and researchers are unwelcome at universities in the US. If not addressed, these consequences will impact dramatically the ability of research universities to conduct fundamental research and enable scientific discovery.

Academic stakeholders must work with the government to address these concerns, a task best accomplished by changing the narrative to security-based rather than foreign entity–based. This shift in perspective will allow everyone to focus on the problem rather than the players, which will create a robust system to address issues from multiple threats rather than one or two isolated foreign entities. These solutions also have to contend with the fact that the academic and research landscape, as well as the global climate, have changed significantly over the last several decades. The US is no longer the clear leader in all areas of scientific knowledge. The Internet greatly enables collaboration and also creates threat vectors through which technology and information can be stolen from a distance and in a skillful manner. The US is facing a research talent shortage and depends on foreign students and research staff to conduct fundamental research. Working together, the government and academia can address this complex problem by first acknowledging its existence and framing the issue properly. The utmost care must be taken to preserve the ability to exchange information freely and conduct the fundamental research that drives innovation, the sharing of knowledge, and the creation of IP—the cornerstone of scientific discovery. Failing to do so would be disastrous for the advancement of knowledge and the US economy.

References

AAU & APLU. 2019. "Actions being taken by universities to address growing concerns about security threats and undue foreign influence on campus." *Unpublished Survey Seport.*

Achenbach, J, B Guarino, S Kaplan, and B Dennis. 2019. *Trump budget seeks cuts in science funding.* March 11. Accessed March 19, 2019. https://www.washingtonpost.com/science/2019/03/11/trump-budget-seeks-cuts-science-funding/?noredirect=on&utm_term=.58ebbf296d86.

Ackerman, Todd. 2018. *Houston Chronicle.* August 8. Accessed February 3, 2019. https://www.houstonchronicle.com/news/houston-texas/houston/article/FBI-warns-Texas-academic-and-medical-leaders-of-13142650.php.

Aguilar, M. 2015. *The number of people who fall for phishing emails is staggering.* April 14. Accessed February 18, 2018. https://gizmodo.com/the-number-of-people-who-fall-for-phishing-emails-is-st-1697725476.

Ahmadpoor, Benjamin F. Jones and Mohammad. 2017. *The Conversation.* August 10. Accessed February 16, 2019. http://theconversation.com/tracing-the-links-between-basic-research-and-real-world-applications-82198.

Ambrose, Mitch. 2018. *American Institute of Physics.* March 16. Accessed February 2, 2019. https://www.aip.org/fyi/2018/us-confronting-threat-chinese-exploitation-intellectual-property.

American Association for the Advancement of Science. n.d. *R&D at Colleges and Universities.* Accessed September 22, 2018. https://www.aaas.org/page/rd-colleges-and-universities.

n.d. *American Association of University Professors.* Accessed February 16, 2019. https://www.aaup.org/report/1940-statement-principles-academic-freedom-and-tenure.

Ascione, L. 2019. *Class of 2019 STEM majors have top salary potential.* January 21. Accessed March 15, 2019. https://www.ecampusnews.com/2019/01/21/class-of-2019-stem-majors-have-top-salary-potential/.

Association of American Universities. 2015. February. Accessed September 8, 2018. https://www.aau.edu/sites/default/files/%40%20Files/Research%20and%20Scholarship/Why%20University%20Research%20Matters/Basic-Research-Paper.pdf.

—. 2018. *Association of American Universities.* July 24. Accessed September 8, 2018. https://www.aau.edu/sites/default/files/AAU-Files/Key-

Issues/Federal-Budget/Appropriations-Tables/Defense-FY19-Funding-Table.pdf.

Atkinson, R. 2018. *Information Technology & Innovation Foundation.* January. Accessed October 4, 2018. http://www2.itif.org/2018-industry-funding-university-research.pdf?_ga=2.33423674.560265895.1538873661-1885207798.1538873661.

Barhat, Vikram. 2018. *CNBC.* May 4. Accessed October 21, 2018. https://www.cnbc.com/2018/05/04/china-aims-to-steal-us-a-i-crown-and-not-even-trade-war-will-stop-it.html.

Carter, Ashton. 2010. "Memorandum for Secretaries of the Military Departments Subject: Fundamental Research." *Office of the Under Secretary of Defense for Acquisition Technology and Logistics.* May 24. Accessed September 17, 2018. https://research.uci.edu/policy-library/export-control-policies/govt-fundamental-research-policy .

Cimpanu, Catalin. 2018. *China has been 'hijacking the vital internet backbone of western countries'.* October 26. Accessed October 30, 2018. https://www.zdnet.com/article/china-has-been-hijacking-the-vital-internet-backbone-of-western-countries/.

Clinton, William J. 2000. "Executive. Order 13185—To Strengthen the Federal Government-University Research Partnership." *The White House. Washington D.C.* Accessed February 2, 2019.

https://www.govinfo.gov/content/pkg/WCPD-2001-01-01/pdf/WCPD-2001-01-01-Pg3211.pdf.

Coats, Daniel. *STATEMENT FOR THE RECORD WORLDWIDE THREAT ASSESSMENT of the US INTELLIGENCE COMMUNITY.* January 29, 2019. https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community (accessed February 15, 2019).

Cohen, Jon. 2018. "U.S. Blames 'Massive' Hack of Research Data on Iran." Science 359 (6383): 1450. DOI:10.1126/science.359.6383.1450. (accessed February 10, 2019)

CohenMar, Jon. "Massive Cyberhack by Iran Allegedly Stole Research from 320 Universities, Governments, and Companies." Science | AAAS. March 25, 2018. (Accessed February 15, 2019). https://www.sciencemag.org/news/2018/03/massive-cyber-hack-iran-allegedly-stole-research-320-universities-governments-and?r3f_986=https://www.google.com/.

Collins, Francis. 2018. *National Institutues of Health.* August 23. Accessed October 21, 2018. https://www.nih.gov/about-nih/who-we-are/nih-director/statements/statement-protecting-integrity-us-biomedical-research.

n.d. *Cornell Law School.* Accessed February 16, 2019. https://www.law.cornell.edu/cfr/text/32/272.3.

Defense Science Board. 2012. "Report of the Defense Science Board Task Force on Basic Research." *Washington, D.C. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics* . Accessed February 2, 2019. https://www.acq.osd.mil/dsb/reports/2010s/BasicResearch.pdf?zoom_highlight=Defense+Science+Board+task+force+on+very+high+speed+integrated+circuits.

Demchak, Chris C, and Yuval Shavitt. 2018. "China's maxim - Leave no access point unexploited: The hidden story of China Telcome's BGP Hijacking." *Military Cyber Affairs* 3 (1): 1-9. doi:10.5038/2378-0789.3.1.1050.

Department of Defense. 2018. *Annual Report to Congress Military and Security Developments Involving the Peoples Republic of China.* Accessed September 2018, 05. https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF.

—. 1982. "Report of the Defense Science Board Task Force on University Responsiveness." *Office of the Under Secretary of Defense for Research and Engineering.* January. Accessed October 27, 2018. http://www.dtic.mil/dtic/tr/fulltext/u2/a112070.pdf.

—. 1981. "Soviet Military Power." *Defense Intelligence Agency.* October 9. Accessed October 27, 2018. http://edocs.nps.edu/2014/May/SovietMilPower1981.pdf.

Department of Homeland Security. 2018. November 14. Accessed March 17, 2019. https://www.ice.gov/sevis.

DHS. 2014. *Cybersecurity Capability Maturity Model White Paper.* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwi_-uOVrsbgAhUIbq0KHeMIDxsQFjACegQICRAC&url=https%3A%2F%2Fniccs.us-cert.gov%2Fsites%2Fdefault%2Ffiles%2FCapability%2520Maturity%2520Model%2520White%2520Paper.pdf%3FtrackDocs%3DCapab.

—. 2015. *Transportation systems sector cybersecurity framework implementation guidenace.* June 26. Accessed April 10, 2018. https://www.dhs.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf.

Edwards, J. 2016. *U.S. targets spying threat on campus with proposed research clampdown.* May 20. Accessed September 19, 2018. https://www.reuters.com/article/us-usa-security-students-idUSKCN0YB1QT.

Eisenhower, Dwight D. 1953. "Executive Order 10501 Safeguarding Official Information in the Interests of the Defense of the United States ." *The White House. Washington D.C.* . Accessed January 26, 2019. https://fas.org/irp/offdocs/eo10501.htm.

Elifoglu, I, Ivan Abel, and Özlem Taşseven. 2018. "Minimizing insider threat risk wiht behavioral monitoring." *Review of Business* 38 (2): 61-73. https://www.stjohns.edu/academics/schools-and-colleges/peter-j-tobin-college-business/departments-and-faculty/tobin-faculty/review-business-interdisciplinary-journal-risk-and.

Elis, Niv. 2019. *Trump calls for cutting National Science Foundation funding by $1 billion.* March 11. Accessed March 16, 2019. https://thehill.com/homenews/administration/433507-trump-proposes-cutting-national-science-foundation-budget-by-billion-dollars.

Facher, Lev. 2018. *STAT.* December 13. Accessed February 2, 2019. https://www.statnews.com/2018/12/13/nih-report-scrutinizes-role-of-china-in-theft-of-u-s-scientific-research/.

Federal Bureau of Investigation. 2018. "FBI Letter to Disband the National Security Higher Education Advisory Board." *U.S. Department of Justice. Washington D.C.* . February 21. Accessed September 20, 2018. https://democrats-science.house.gov/sites/democrats.science.house.gov/files/documents/FBI

%20Letter%20to%20NSHEAB%20Members%20Disbanding%20Group%20-%202.21.2018.pdf.

FireEye. 2019. *Advanced persistent threat groups.* Accessed February 26, 2019. https://www.fireeye.com/current-threats/apt-groups.html.

Flaherty, Colleen. 2018. *Inside Higher Ed.* May 9. Accessed March 19, 2019. https://www.insidehighered.com/news/2018/05/09/no-clear-solution-nationwide-shortage-computer-science-professors.

Gamache, K. 2018. *Senator Cornyn questions for the record for Dr. Kevin Gamache, Chief Security Officer, Texas A&M University System.* 29 June. Accessed September 8, 2018. https://www.judiciary.senate.gov/imo/media/doc/Gamache%20Responses%20to%20QFRs1.pdf.

—. 2018. "Student visa integrity: Protecting educational opportunity and national security." *Subcommittee on Border Security and Immigration of the Judiciary Committee.* Washington D.C.: U.S. Senate, June 6.

Gelbstein, Ed. 2013. *Quantifying Information Risk and Security.* Accessed December 22, 2018. https://www.isaca.org/Journal/archives/2013/Volume-4/Pages/Quantifying-Information-Risk-and-Security.aspx?utm_referrer=.

Gillin, Donald G. 1965. “China’s First Five-Year Plan: Industrialization under the Warlords as Reflected in the Policies of Yen Hsi-Shan in Shansi Province, 1930-1937." The Journal of Asian Studies Vol 24 no (2): pg 245-259. DOI: 10.2307/2050564. (accessed October 22, 2018).

Grassley, Charles E. 2018. *Letter from Senator Charles E. Grassley to Dr. Francis Collins.* October 13. Accessed November 5, 2018. https://www.grassley.senate.gov/sites/default/files/constituents/2018-10-23%20CEG%20to%20NIH%20(Research%20Threats).pdf.

Greenberg, Daniel. 2003. *The Scientist.* March 24. Accessed February 23, 2019. https://www.the-scientist.com/closing-bell/the-mythical-scientist-shortage-51906.

Guarino, B., E. Rauhala, and W. Wan. 2018. *The Washington Post.* June 3. Accessed October 7, 2018. https://www.washingtonpost.com/national/health-science/china-challenges-american-dominance-of-science/2018/06/03/c1e0cfe4-48d5-11e8-827e-190efaf1f1ee_story.html?noredirect=on&utm_term=.d0db8e6b025f.

Gupta, A, and H Wang. 2016. *Harvard Business Review.* November 16. Accessed November 6, 2018. https://hbr.org/2016/11/how-chinas-government-helps-and-hinders-innovation#comment-section.

Haas, L J. 2018. *Passing the torch to China.* March 6. Accessed September 5, 2018. https://www.usnews.com/opinion/world-report/articles/2018-03-06/global-power-is-shifting-from-the-us-to-china.

Halbert, Deborah. 2016. "Intellectual property theft and national security: Agendas and assumptions." *The Information Society* 32 (4): 256-268. doi:10.1080/01972243.2016.1177762.

Hampson, M. 2018. *Publicly-funded Research Lays Critical Foundation for Private Sector.* March 30. Accessed September 20, 2018. https://www.aaas.org/news/publicly-funded-research-lays-critical-foundation-private-sector.

Harnedy, R. 2016. *3 better ways to use backup to recover from ransomeware.* https://blog.barkly.com/3-better-ways-to-use-backup-to-recover-from-ransomware.

Hartig, Falk. 2015. "Communicating China to the World: Confucius Institutes and China's Strategic Narratives." Politics Vol 35, no.(3-4): pg 245-258. DOI: 10.1111/1467-9256.12093. (accessed September 10, 2018).

Homer, A N, T L Smith, and J B McCormick. 2008. *Beyond Sputnik.* Ann arbor: University of Michigan Press. doi:10.3998/mpub.22958.

Hourihan, M. 2018. *American Association for the Advancement of Science.* June 18. Accessed September 29, 2018. https://www.aaas.org/news/defense-funding-notes-darpa-house-shifts-away-other-research.

Howard, D. 2013. *Issues in Science & Technology.* Accessed October 5, 2018. https://issues.org/the-new-normal-in-funding-university-science/.

Hoy, Anne Q. 2018. *American Association for the Advancement of Science.* August 31. Accessed September 29, 2018. http://science.sciencemag.org/content/361/6405/861?__utma=109413082.1091763610.1537636838.1538269849.1538275721.5&__utmb=109413082.1.10.1538275721&__utmc=109413082&__utmx=-&__utmz=109413082.1538244896.3.2.utmcsr=google%7Cutmccn=(organic)%7Cutmcmd=organic%7Cutmctr=(not%20provided)&__utmv=-&__utmk=49594150.

Impe, Koen Van. 2018. *Simplifying Risk Management.* March 28. Accessed December 22, 2018. https://securityintelligence.com/simplifying-risk-management/.

2019. *International Student.* Accessed March 17, 2019. https://www.internationalstudent.com/immigration/f1-student-visa/.

Jesson, J, L Mattheson, and F Lacey. 2011. *Doing Your Literature Review.* Los Angeles: Sage Publications Ltd.

Jia, Hepeng. 2018. "China's Plan to Recruit Talented Researchers." Nature, Vol 553 no. (7688). http://www.nature.com.ezproxy.library.tamu.edu/magazine-assets/d41586-018-00538-z/d41586-018-00538-z.pdf. (accessed September 17, 2018).

Jia, Hepeng. 2018. *Nature Index.* March 23. Accessed November 6, 2018. https://www.natureindex.com/news-blog/chinas-science-ministry-gets-power-to-attract-more-foreign-scientists.

Kaiser, J. 2008. *Senate Inquiry on Research Conflicts Shifts to Grantees.* August 22. Accessed October 6, 2017. http://science.sciencemag.org.ezproxy.library.tamu.edu/content/320/5884/1708.

Kakuchi, S. 2018. *As funding falls, China emerges as key research partner.* April 27. Accessed September 15, 2018. http://www.universityworldnews.com/article.php?story=20180425150957877.

Karagianis, Liz. 2014. *MIT Spectrum.* Accessed February 16, 2019. https://spectrum.mit.edu/spring-2014/the-brilliance-of-basic-research/.

Kenderdine, Tristan. 2017. *Asian Scientist.* October 17. Accessed November 6, 2018. https://www.asianscientist.com/2017/10/features/china-science-technology-funding/.

Khisamutdinov, A. A. 2016. “Russian Higher Education in China.” Russian Education & Society Vol 58 no (7): pp 471–90. DOI: 10.15448/1981-2582.2017.3.28799 (accessed October 22, 2018).

Kim, Y. 2018. *The importance of literature review and research writing.* January 11. https://owlcation.com/humanities/literature_review.

Lawder, David. 2016. *U.S. keeps China, India on intellectual property shame list.* April 27. Accessed October 21, 2018. https://www.reuters.com/article/us-usa-trade-ip-idUSKCN0XO1IT.

Leiber, Nick. 2018. “Visa Headaches Discourage Foreign Applicants to U.S Business Schools.” Bloomberg Businessweek. https://www.bloomberg.com/news/articles/2018-11-08/visa-headaches-discourage-foreign-applicants-to-u-s-b-schools (accessed November, 7th 2018).

Li, P, X Yang, Q Xiong, J Wen, and Y Tang. 2018. "defending against the advanced persistent threat: An optimal control approach." *Security and Communication Networks* 2018: one through 14. doi:https://doi.org/10.1155/2018/2975376.

Llorente, E. 2019. *Chinese accused of stealing biomed research from U.S. labs, universities.* January 7. Accessed March 16, 2019. https://www.foxnews.com/science/chinese-stealing-biomedical-research-from-u-s-labs-and-universities.

Loudenback, T. 2016. *International students are now 'subsidizing' public American universities to the tune of $9 billion a year.* September 16. Accessed September 13, 2018. https://www.businessinsider.com/foreign-students-pay-up-to-three-times-as-much-for-tuition-at-us-public-colleges-2016-9.

Martinson, B, A. Crain, M. Anderson, and R. De Vries. 2009. *National Center for Biotechnology Information, U.S. National Library of Medicine.* November. Accessed October 6, 2018. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3071700/.

Mattis, Jim. 2018. "National Defense Strategy of The United States of America." *Department of Defense* . January 19. Accessed October 30, 2018. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf .

McGuire, M. 2018. "Into the web of profit." *Bromium.* April. Accessed February 26, 2019. https://learn.bromium.com/rprt-web-of-profit.html.

McLaughlin, Kelly. 2018. *Business Insider.* July 24. Accessed February 2, 2019. https://www.businessinsider.com/chinese-billionaire-is-accused-of-stealing-research-from-a-duke-lab-2018-7.

Mervis, Jeffrey. 2017. *American Association for the Advancement of Science.* March 9. Accessed September 8, 2018. http://www.sciencemag.org/news/2017/03/data-check-us-government-share-basic-research-funding-falls-below-50.

Metz, C. 2018. *The net tech talen shortage: Quantum computing researchers.* October 21. Accessed February 18, 2019. https://www.nytimes.com/2018/10/21/technology/quantum-computing-jobs-immigration-visas.html.

Mitchell, Ted. 2018. "Letter to FBI Director Wray re: National Security Higher Education Advisory Board." *American Council on Education.* April 24. Accessed September 18, 2018. https://www.acenet.edu/news-room/Documents/Letter-FBI-NSHEAB.pdf.

Morgan, S. 2017. *Cybersecurity Business Report.* Novermber 20. https://www.csoonline.com/article/3237674/ransomware/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html.

National Academies of Sciences, Enginneering, and Medicine. 2016. *Optimizing the Nation's Investment in Academic Research: A New Regulatory Framework for the 21st Century.* Washington, DC: The National Academy Press. doi:10.17226/21824.

National Academy of Sciences. 1982. "Scientific Communication and National Security." *Washington, DC: The National Academies Press.* Accessed September 19, 2018. https://www.nap.edu/download/253.

National Institutes of Health. 2018. *Budget.* April 11. Accessed September 13, 2018. https://www.nih.gov/about-nih/what-we-do/budget.

National Science Board . 2018. *Science & Engineering Indicators 2018.* January. Accessed September 29, 2018. https://www.nsf.gov/statistics/2018/nsb20181/report.

National Science Board Science & Engineering Indicators 2018. 2018. *Academic Research & Development.* January. Accessed September 29, 2018.

https://www.nsf.gov/statistics/2018/nsb20181/report/sections/academic-research-and-development/expenditures-and-funding-for-academic-r-d.

Newman, Lily. 2018. *The Worst Cybersecurity Breaches of 2018 So Far.* July 09. https://www.wired.com/story/2018-worst-hacks-so-far/.

NIH Advisory Committee to the Director. 2018. *National Institutes of Health.* December. Accessed February 16, 2019. https://acd.od.nih.gov/documents/presentations/12132018ForeignInfluences_report.pdf.

Nihco, M, H Fakhry, and E Uche. 2018. "evaluating user vulnerabilities vs phisher skills and spear phishing." *IADIS International Journal on Computer Science and Information Systems* 13 (2): 93-108. IADIS International Journal on Computer Science and Information Systems.

“Nine Iranians Charged with Massive Cyber Theft.” 2018. Computer & Internet Lawyer 35 (6): 24–25.file:///home/chronos/u-4f52f93ab957db10cf08834b85635dc494f937d7/Downloads/ContentServer.pdf (accessed February 15, 2019)

NIST. 2017. *Capability Maturity Model Integration (MMI).* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwi_-uOVrsbgAhUIbq0KHeMIDxsQFjABegQIChAC&url=https%3A%2F%2Fcsrc.nist.gov%2FCSRC%2Fmedia%2FProjects%2FSupply-Chain-Risk-

Management%2Fdocuments%2Fssca%2F2017-winter%2FTueAM2_2_CMMI.pdf.

Normile, D. 2018. *American Association for the Advancement of Science.* June 5. Accessed October 7, 2018. http://www.sciencemag.org/news/2018/06/generous-funding-and-top-tier-jobs-china-seeks-lure-science-talent-abroad.

Norris, Julie T. 2003. *Restrictions on research awards: Troublesome clauses.* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwjw-uaKvcXgAhURC6wKHZWpC_IQFjAHegQIAxAC&url=https%3A%2F%2Fwww.aau.edu%2Fsites%2Fdefault%2Ffiles%2FAAU%2520Files%2FKey%2520Issues%2FScience%2520%2526%2520Security%2FReport_AAU-COGR_R.

Office of the Director Defense Research and Engineering. 1976. "An Analysis of Export Control of U.S. Technology – A DOD Perspective. A Report of the Defense Science Board Task Force on Export of U.S. Technology." *Washington D.C. Department of Defense.* Accessed January 08 , 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/a022029.pdf.

OPM. 2019. *CyberCorps®: Scholarship for Service.* https://www.sfs.opm.gov/.

Osborne, C. 2018. *Irani and hackers target 70 universities worldwide to steal research.* August 24. Accessed February 26, 2019.

https://www.zdnet.com/article/iran-hackers-target-70-universities-in-14-countries/.

PhishMe. 2016. *Enterprise Phishing Susceptibility and Resiliency Report.* Leesburg: PhishMe. https://phishme.com/enterprise-phishing-susceptibility-report.

Posen, Adam. 2018. "Economics-based Principles for a post-conflict China-US commercial regime." *China & World Economy* 2 (11): 2-11. doi:10.1111/cwe.12253.

Prableen, B. 2019. "The world's top 20 economies." *Investopedia.* January 10. Accessed February 26, 2019. https://www.investopedia.com/insights/worlds-top-economies/.

Qian, Zhu. 2015. “From the First Five-Year Plan to the Cultural Revolution: The Pre-Reform Urban Transformation of Hangzhou, China.” *Planning Perspectives* Vol 30 no (4): pg 571–95. DOI: 10.1080/02665433.2014.995694. (accessed October 3, 2018).

Redden, Elizabeth. 2018. *Chinese students: Security Threat or Sterotype Threat.* June 7. Accessed September 14, 2018. https://www.insidehighered.com/news/2018/06/07/lawmakers-discuss-national-security-concerns-and-chinese-students.

Riechmann, Deb. "US Braces for Possible Cyberattacks after Iran Sanctions." Military Times. August 08, 2018.

https://www.militarytimes.com/flashpoints/2018/08/08/us-braces-for-possible-cyber-attacks-after-iran-sanctions/ (accessed February 15, 2019).

Reisch, Marc. 2018. *Chemical & Engineering News.* June 27. Accessed February 2, 2019. https://cen.acs.org/policy/intellectual-property/Acknowledging-spies-campus/96/i27.

Remedios, Cris dos. 2006. *International Union for Pure and Applied Biophysics.* Accessed February 16, 2019. http://iupab.org/publications/value-of-fundamental-research/.

Rice, Condoleezza. 2001. "Secretary Condoleezza Rice's 2001 reaffirmation of NSDD-189." *The White House Washington D.C.* . Accessed September 19 , 2018 . https://fas.org/sgp/bush/cr110101.html.

Riggi, John. 2018. *American Hospital Association.* April 24. Accessed February 2, 2019. https://www.aha.org/news/blog/2018-04-24-nation-state-cyber-threats-targeting-intellectual-property.

Ross, M. 2018. *Spy Theft of U.S. University Research Sparks Call for Action.* April 12. Accessed September 5, 2018. https://clayhiggins.house.gov/media/in-the-news/spy-theft-us-university-research-sparks-call-action.

Saady, Brian. 2018. *The unreal scope of China's intellectual property theft.* July 23. Accessed October 21, 2018.

https://www.theamericanconservative.com/articles/the-unreal-scope-of-chinas-intellectual-property-theft/.

Sample, I. 2017. *'We can't compete': Why universities are losing their best AI scientists.* November 1. Accessed Februrary 18, 2019. https://www.theguardian.com/science/2017/nov/01/cant-compete-universities-losing-best-ai-scientists.

Sargent Jr., J. 2018. *U.S. Research and Development Funding and Performance: Fact Sheet.* June 29. Accessed September 20, 2018. https://fas.org/sgp/crs/misc/R44307.pdf.

Schultze, H. 2018. *2018 Insider Threat Report.* Accessed February 26, 2019. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwjwkPP8lNrgAhUOPa0KHWZxByoQFjACegQIBhAK&url=https%3A%2F%2Fwww.ca.com%2Fcontent%2Fdam%2Fca%2Fus%2Ffiles%2Febook%2Finsider-threat-report.pdf&usg=AOvVaw0MjU5J9iDtekck3osz2gCu.

Sharma, Y. 2018. *University World News.* March 21. Accessed October 7, 2018. http://www.universityworldnews.com/article.php?story=2018032117551180.

Shoebridge, Michael. 2018. *China's militaryhas one aim in sending its scientists to study in the west.* October 31. Accessed October 31, 2018.

https://www.realcleardefense.com/articles/2018/10/31/chinas_military_has_one_aim_in_sending_its_scientists_to_study_in_the_west_113924.html.

Showstack, R. 2018. *EOS Earth & Space Science News.* February 20. Accessed September 20, 2018. https://eos.org/articles/china-may-soon-surpass-the-united-states-in-rd-funding.

—. 2018. *EOS Earth & Space Science News.* January 24. Accessed October 7, 2018. https://eos.org/articles/china-catching-up-to-united-states-in-research-and-development.

South China Morning Post. 2018. *South China Morning Post.* February 27. Accessed November 6, 2018. https://www.scmp.com/news/china/policies-politics/article/2134895/chinas-spending-research-and-development-14pc-2017.

Sun, L. and Cheng, Y. (2014) ‘Confucius Institute May Diversify Funding,’ *China Daily, 9 December*, p. 1. DOI 10.1111/1467-9256.12093 (accessed October 3, 2018).

Suttmeier, R. 2018. *Scientific American.* June 29. Accessed November 6, 2018. https://www.scientificamerican.com/article/how-china-is-trying-to-invent-the-future-as-a-science-superpower/.

Tang, Y. (2010) ‘Education: Confucius Teaching Chinese Abroad,’ Beijing Review, 7 January. Available from:

http://www.bjreview.com.cn/life/txt/2010-01/04/content_237885.htm (accessed February 15, 2010).

Tankard, C. 2011. "Advanced persistent threats and how to monitor and deter them." *network security* 2011 (i): 16 – 19. doi:https://doi.org/10.1016/S1353-4858(11)70086-1.

The National Bureau of Asian Research. 2017. *Update to the IP Commission Report.* Accessed September 4, 2018. http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf.

The White House. 1985. "National Security Decision Directive 189 National Policy On The Transfer Of Scientific, Technical And Engineering Information." Accessed September 06, 2018. https://www.aau.edu/sites/default/files/AAU%20Files/Key%20Issues/Science%20%26%20Security/Memo_DOD-NSDD-189_2008.pdf.

Thomas, J E. 2017. "Lessons learned in management, marketing, sales, and finance incentive practices a decade after the Subprime Mortgage Crisis." *International Journal of Business and Management* 12 (3): 19-26. doi:10.5539/ijbm.v12n3p19.

Thomas, J E. 2018. "Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks." *International Journal of Business and Management* 13 (6): 1-24. doi:10.5539/ijbm.v13n6p1.

Thomas, J E, and G C Galligher. 2018. "Improving backup system evaluations in information security risk assessments to combat ransomware." *Computer and Information Science* 11 (1): 14-25. doi:10.5539/cis.v11n1p14.

Thomas, J E, and P E Hornsey. 2014. "Adding rigor to classroom assessment techniques for non-traditional adult programs: A lifecycle improvement approach." *Journal of Instructional Research* 3: 27-37. https://cirt.gcu.edu/jir.

Timmons, Heather. 2018. *The US's newest partner in fighting Chinese intellectual property theft is Taiwan.* November 1. Accessed November 5, 2018. https://qz.com/1447913/the-us-is-partnering-with-taiwan-to-fight-chinas-intellectual-property-theft/.

Trump, Donald. 2017. "The National Security Strategy of the United States of America." *The White House Washington D.C.* . Accessed October 30, 2018. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf. .

U.S. Central Intelligence Agency. 1982. "Soviet Acquisition of Western Technology and its National Security Implications." February 23. Accessed October 27, 2018 . https://www.cia.gov/library/readingroom/docs/CIA-RDP83M00914R002000070021-4.pdf.

University of Michigan. 2017. *Phys Org.* June 15. Accessed October 7, 2018. https://phys.org/news/2017-06-science-china-rose-fast-funding.html.

Weeks, Jennifer. 2015. *Science History Institute.* Accessed February 23, 2019. https://www.sciencehistory.org/distillations/magazine/shortage-or-surplus.

Wilday, T M. 2018. *Comparing and contrasting how the United States and China address cybersecurity.* Accessed 2019. https://search.proquest.com/openview/e53c0ca72156227c8d449d451c0855c8/1?pq-origsite=gscholar&cbl=18750&diss=y.

Young, John. 2008. "Contracted Fundamental Research." *The Under Secretary of Defense for Acquisition, Technology And Logistics.* Accessed September 06, 2018. https://www.aau.edu/sites/default/files/AAU%20Files/Key%20Issues/Science%20%26%20Security/Memo_DOD-NSDD-189_2008.pdf.

Zhu, Kaixuan. 1997. “Tentative Ideas Regarding the Ninth Five-Year Plan for China’s Education and Its Long-Term Targets for the Year 2010, November 20, 1995.” *Chinese Education & Society* Vol 30 no (3): pg 7–28. DOI 10.2753/CED1061-193230037. (accessed October 4, 2018).