

# “The Man Who Removes a Mountain Begins by Carrying Away Small Stones”

## Addressing Chinese Exploitation of U.S. Education Systems

Amanda Goyeneche Theus

Master Sgt. Robert Theus, U.S. Army



*The man who removes a mountain begins by carrying away small stones.*

—Proverb

China has embarked on an ambitious initiative coined “Made in China 2025,” pledging to lead global efforts in microtechnologies and artificial intelligence, among other science, technology, engineering, and math (STEM) developments. China’s actions are considered to be part of what is known as unrestricted warfare, as discussed in John Van Messel’s master’s thesis “Unrestricted Warfare: A Chinese Doctrine for Future Warfare?” They are a way for China to compete with the United States through economic advancements and the internet rather than through traditional military means.<sup>1</sup>

Along with deep learning and artificial intelligence, our nation’s universities are leading the charge on innovation and creating technology with insurmountable outcomes. As noted by Will Knight, “We’ve never before built machines that operate in

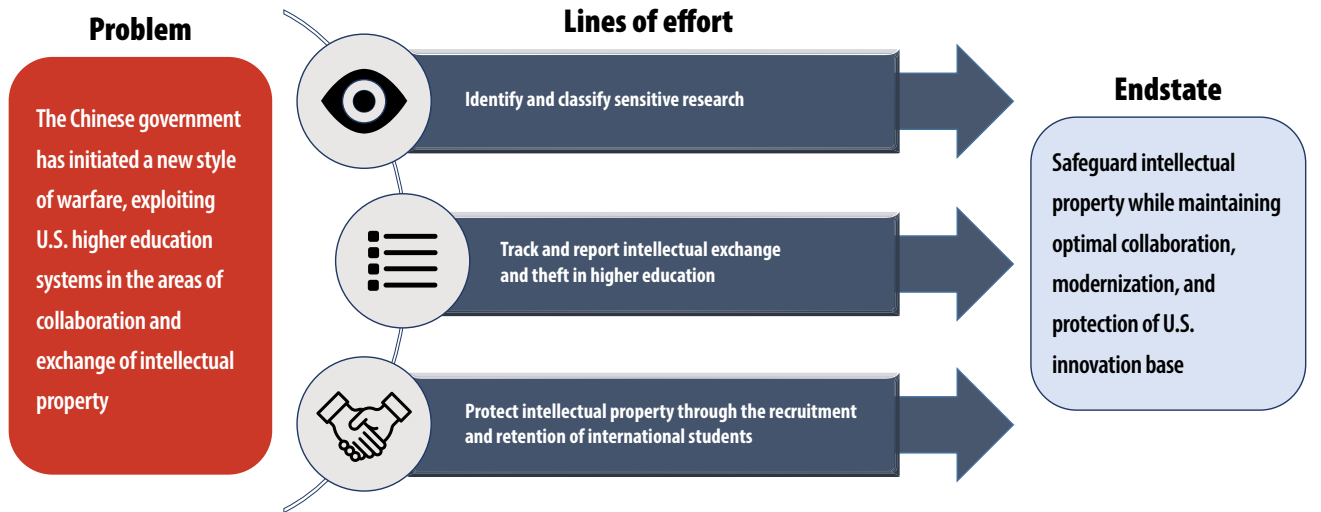
ways their creators don’t understand.”<sup>2</sup> These advancements spawned in academia are targeted by the Chinese, who see their procurement by any means as a shortcut to catching up with U.S. technology. Therefore, understanding the threats and possible strategies that China is employing and safeguarding the intellectual property gained at the institutional level has

### Amanda Goyeneche

**Theus** is an instructional systems specialist for the Department of the Army and serves as a civilian instructor and training developer for faculty and staff at the Fires Center of Excellence in Fort Sill, Oklahoma. She holds a EdM in educational media and technology from Boston University and a BA in education from Coker University.

### Master Sgt. Robert Theus, U.S. Army,

serves as the 13Z career manager in the Field Artillery Proponent Office at Fort Sill, Oklahoma. He is working on an associate degree in military history from the American Military University and has interests in military theory, strategy, and tactics.



(Graphic by authors; icons courtesy of Freepik, [freepik.com](https://www.freepik.com))

**Figure. Intellectual Advancement and Protection Strategy**

a definite place among tried and true military tactics and strategies (see figure).

The *National Security Strategy of the United States of America* outlines the need for examining new ways to address the potential threat from China, citing a clear concern over the current prevention methods. The government has taken careful measures to safeguard work with partnering industries, but the same cannot be said for the early innovation cultivated within academia. The need to protect and preserve intellectual property leads to increased motivation to maintain the highest quality of recruitment efforts across academia, industry, and government; and a mass of newly generated systems and intellectual properties are being exchanged at the higher education level. This unmonitored flow of information puts us in a compromising position and demonstrates the need to put forth solutions that are both purposeful and systematic to protect our nation's interests at the source of research and collaboration.

By taking lessons learned from the military, we can safeguard our intellectual property as a top priority through multiple lines of effort that identify, track, and protect our education systems from our country's adversaries.

### What Does the Data Say?

According to the Defense Security Service, a Department of Defense agency that protects American technology, a staggering 24 percent of

foreign efforts to obtain information in 2014 appeared in the form of academic solicitation or "the use of students, professors, scientists, or researchers as collectors."<sup>3</sup> So we must ask ourselves, where does our intellectual property go during and after academic research? Do we really know where our university students are going, and what they are doing with all the knowledge and partnerships they have gained? We honestly do not know the whole picture; we do not have a solid means of tracking intellectual information gained from research universities, let alone what happens to it once a foreign student or professor involved in such research returns to his or her home country.

Professional educators know that their success is tracked by their alma maters years after completing their requirements for graduation. Their certification scores, evaluations, professional development, and contribution to the field of education remain directly tied to their schools' accreditation and, ultimately, the schools' ability to recruit and retain similar high-performing students and eventual graduates. In addition, each university follows its own guiding principles for program evaluation along with accreditation guidance. Unfortunately, this makes it difficult to see standardization or possible tracking solutions that fit across a universe of professorial protocol.

We can, however, learn lessons by examining past cases of espionage, such as that of Zhang Hao in



2015. Zhang was arrested and indicted after a decade-long process of stealing information and processes on microelectronics from the United States. He was a Chinese professor who studied and worked in the United States while stealing sensitive information to establish his own university and business programs to develop technology as part of a billion-dollar-a-year business.<sup>4</sup> The U.S. government investigation determined that Zhang had been executing his plan for a long period of time through trusted collaboration all the way to the university level.

To avoid future situations similar to that of Zhang, academic professionals must understand and define intellectual property and determine whether it could potentially be used to compete with U.S. economic interests or, in a worst-case scenario, present itself as a national security concern. A major challenge ahead stems from defining intellectual property. This task requires multiple partners and entities to engage in and establish left and right limits for defining intellectual property and any potential impact.

## Proposed Solutions


To use the overarching Chinese proverb of small “stones” as an analogy for potential solutions, we cannot fence off our academic mountain completely. That would be both impossible and impractical. The students providing valuable research work and the collegiality and empowerment being forged by university collaboration are absolutely necessary for our country to keep moving



# WANTED BY THE FBI

## APT 10 GROUP

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud;  
Aggravated Identity Theft

ZHU HUA
ZHANG SHILONG

DETAILS

On December 17, 2018, a grand jury in the United States District Court for the Southern District of New York indicted ZHU HUA, aka “Afwar,” aka “CVNX,” aka “Alayos,” aka “Godkiller,” and ZHANG SHILONG, aka “Baobeilong,” aka “Zhang Jianguo,” aka “Atreexp,” two members of a hacking group operating in China known in the cybersecurity community as Advanced Persistent Threat 10 (the “APT 10 Group”), with conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft. The defendants worked for Huaying Haitai Science and Technology Development Company located in Tianjin, China, and they acted in association with the Chinese Ministry of State Security’s Tianjin State Security Bureau.

As alleged in the Indictment, from at least 2006 through 2018, the defendants conducted extensive campaigns of global intrusions into computer systems aiming to steal, among other data, intellectual property and confidential business and technological information from more than at least 45 commercial and defense technology companies in at least a dozen states, managed service providers (“MSP”), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, and U.S. government agencies. The victim companies targeted by ZHU HUA and ZHANG SHILONG were involved in a diverse array of commercial activity, industries, and technologies, including aviation, space and satellite technology, manufacturing technology, oil and gas exploration, production technology, communications technology, computer processor technology, and maritime technology. In addition, for example, the APT 10 Group’s campaign compromised the data of an MSP and certain of its clients located in at least 12 countries including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The APT 10 group also compromised computer systems containing information regarding the United States Department of the Navy and stole the personally identifiable information of more than 100,000 Navy personnel.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

An FBI wanted poster depicts two Chinese nationals accused of hacking more than forty-five commercial and defense technology companies. The authors assert that companies should learn lessons from the military regarding how to protect intellectual property. (Poster courtesy of the Federal Bureau of Investigation)

ahead with innovation in every single field. Students bring “stones” of their own that solidify our mountain, growing it in ways that would not be possible any other way. As for the “stones” being taken away, we cannot prevent students from obtaining knowledge and taking intellectual information elsewhere to competing countries or any country for that matter. That is, after all, why many international students come to the United States—to empower themselves to make changes in their respective corners of the globe.

There is no single solution that will work to stop intellectual property theft. Instead, rather than resort to apparent and extreme xenophobic vetting (a practice quite far from the true American spirit), we must employ multiple lines of effort to begin combatting such





actions. We can mitigate risks as best as we can while promoting and protecting our innovation base by using some of the best technology and practices available. Each line of effort must be valid, reliable, and practical if we plan on being successful.

**Line of effort: Identify and classify sensitive research.** The first line of defense is to know what is and would be at risk in the first place. This is easier said than done for a multitude of reasons. Much of the research and technological developments occurring in academia have not been identified by the government or the military for the use of national security or defense. Daniel Golden, author of *Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities*, addresses quite a few stories of espionage and the historical and ongoing exploitation of U.S. education systems. We do know that “almost two-thirds of all economic espionage cases alleging a foreign destination for stolen trade secrets involve China.”<sup>5</sup> Although the emphasis of the book is targeted at our own use and misuse of intelligence rampant throughout key higher-education institutions, Golden introduces several similar case studies like that of

Liu Ruopeng, chairman of KuangChi Science, presents the Kuang-Chi Martin Jetpack at a KuangChi Global Innovators meeting 20 July 2015 in Shenzhen, Guangdong Province, China. (Photo by Mao Siqian, Xinhua, Alamy Live News)

Liu Ruopeng, who sold intellectual property and opened facilities to Chinese colleagues in a series of misguided attempts to steal practices and processes. In that instance and in hindsight, Liu's former professor, David Smith, was quoted as saying, “No one has any training in intellectual property. It's something we're all grappling with—where to draw the line.”<sup>6</sup> At the same time, many universities actively seek out funding and project coordination with the military for research that has very particular protocols for safeguarding information. This line of effort focuses entirely on identifying and classifying our intellectual property. Essentially, we need to examine what “stones” we have, how many we have, how important they are, and how vulnerable they are to being taken.

Within a decade, we have increased active-shooter training in universities tenfold. We should apply the



“ If we take practices from DARPA and help train universities to self-identify, classify, and stay vigilant about our partners and research, we can start building proactive prevention practices to protect intellectual property. ”

same care and caution to integrating inclusive community and intellectual property training into academia. Embedding training and guidance on insider threats as well as incorporating relevant and appropriate government or military policy would help to alleviate some of the concern that higher education may face with the development of sensitive research.

As discussed in *Spy Schools*, much of the collaboration among students, faculty, and fellow international institutions is unwritten, without formal limitations or agreements that are clearly defined.<sup>7</sup> A lesson we can learn from the military involves examining the levels of foreign disclosure among military centers of excellence across the nation. For every program of instruction, we know who can or cannot be in that instruction or part of that collaboration based on our international relationships and agreements. There are levels of foreign disclosure associated with the classification of documents and locations that help create a standardization.

Another essential part of this first line of effort extends past training on intellectual property to the understanding of sensitive information. There is no doubt that we collaborate with a number of partners at the university level, providing the ultimate breeding ground for unprecedented and innovative work. A big part of that includes the responsibility of faculty and students to know when they are engaging in or even stumbling upon something that has the potential to endanger lives if put into the hands of our nation's adversaries. At the lowest level, students within any program, STEM especially, need to be knowledgeable of the dangers inherent in their work and how to identify and report suspicious activity. We have to prioritize specific universities and programs, and use pilot programs that encourage identification and reporting as a means to start building a database for examination and development of best practices to implement elsewhere.

The Defense Advanced Research Projects Agency (DARPA) can show us a lot when it comes

to collaboration with sensitive and groundbreaking information. The organization refers to university collaborators as part of an ecosystem of innovation, providing multiple pathways and incentives embedded within collaborative work.<sup>8</sup> Historically, DARPA has been a catalyst for growing highly impactful defense research with a huge scope and footprint. Examples of DARPA's work include including improvements on the standard M16 rifle in the 1960s, to the Lockheed Have Blue, the first practical combat stealth aircraft in the 1970s and 1980s, to the very recent transfer of work to the Office of Naval Research on the Sea Hunter, a new unmanned surface vehicle that is capable of traveling across great distances of water without any crew. These examples and many other unprecedented projects greatly affect our soldiers on the battlefield today. With so much at stake regarding our ability to obtain and hold a strategic advantage, it makes sense for DARPA to clearly outline projects, permissions, clearances, and protocol for engaging in research projects. DARPA also delineates between fundamental research and the dissemination of research that could jeopardize national security, including work that is tied to military systems or manufacturing technologies.<sup>9</sup>

STEM programs within universities are not operating with the same awareness, knowledge base, or protocol to identify sensitive information or define and designate fundamental research. If we take practices from DARPA and help train universities to self-identify, classify, and stay vigilant about our partners and research, we can start building proactive prevention practices to protect intellectual property that may be leveraged against us.

**Line of effort: Track and report intellectual exchange and theft in higher education.** Identifying best practices for avoiding intellectual property theft happens only after we collect data on how universities are, in fact, collecting data on intellectual property. Studying universities' efforts with regard to



“If users have to submit requests to gain more access, it becomes easier to track areas that have been identified as sensitive or of high interest based on specific priorities and to track the information requested by organizations or individuals.”

intellectual theft and espionage is supported within the *National Security Strategy*.<sup>10</sup> However, as with most strategic-level documents containing intellectual property and regulatory guidance, practical implementation and execution directions are not often provided. Fortunately, DARPA again shows us how technology can provide a means to achieve the type of analytics needed for tracking and reporting.

DARPA uses Polyplexus, an online, social collaboration platform, which aims for research-and-development productivity and encourages micropub portfolios and contribution from similar projects to working experts in an “incubator environment,” “where startup businesses and concepts can be developed without the pressure for instant revenue generation in the marketplace.”<sup>11</sup> DARPA’s mission, “Shape the questions that shape the future,” demonstrates the collaborative nature of the multiple organizations involved in compound levels of research.<sup>12</sup> Importantly, the fact that all of this collaboration occurs within an online social media platform allows for examination of trends and quantifiable data to help determine what is being paid attention to, what it is being used for, and the potential for its future development and further collaboration.

A similar platform should be used for universities in a cooperative consortium, enabling faculty and even students to track and report the movement of intellectual property while working. The multiple levels of Polyplexus allow for individual users to collaborate based on their level of interest and partnership, similar to the government’s adherence of “For Official Use Only” material. If users have to submit requests to gain more access, it becomes easier to track areas that have been identified as sensitive or of high interest based on specific priorities and to track the information requested by organizations or individuals.

Machine learning has become an important way of using technology to enhance our ability to look at information in a more analytical and efficient way in order to make informed decisions. One of the challenges of new

systems is understanding how machines can come to a particular result or solution. However, achieving this understanding introduces an element of trust between humans and machines, making it less difficult for users to embrace widespread technological use.

Our government currently uses systems that monitor and report fraud, waste, and abuse.<sup>13</sup> The system gets “smarter” the more transactions it encounters, identifying patterns and trends that are otherwise missed. This ability also adds to the validity and consistency of reports as well as potential or proposed changes.

If we employ machine learning to a social research online platform, systems can alert us to potential misuse of intellectual property by taking the unseen parts of collaboration and making them visible far quicker and with a wider scope than a highly trained individual could. Reporting and following structured protocol then becomes more effective, and these systems could be implemented across multiple universities or collaborative programs. Incorporating operative training systems makes tracking and reporting more valid, reliable, and practical for all partners involved.

**Line of effort: Protect intellectual property through the recruitment and retention of international students.** This nation’s universities have some of the best research reputations the world can find. In 2012–13, nearly 60 percent of engineering doctorates conferred by U.S. universities were earned by international students.<sup>14</sup> Although this helps our nation build highly revered researchers, practices, and technological developments, it also increases the risk for malicious behavior by our adversaries. As outlined in the *National Security Strategy*, there is no true way to eliminate all the threats that are present in our universities. However, we can still work toward mitigating as many risks as we can through recruiting and retaining the most innovative students regardless of their nationality. To better understand the strategies we need to implement, we must examine



current and best practices across universities regarding recruitment and retention.

As a top university, Stanford is highly sought after for robust, life-changing scholastic pursuits. Situated less than fifteen miles from the ever-expanding Silicon Valley, Stanford remains on the cutting edge of technological research and development. Along with many other highly esteemed universities, the institution hosts many international students and actively seeks out diversity across its programs. The Chinese Undergraduate Visiting Research Program, in partnership with the Stanford School of Engineering, brings multiple Chinese students into

training along with successful university practices, we can start to piece together a legitimate process for universities and organizations to use that would mitigate some of the known risks with encouraging global collaboration.

We should also take care to avoid too many restrictions on international students. We could lose some of the best research contributors as well as increase the likelihood that students feel unwelcome through the pressure of being regarded as possible espionage or insider threats. There needs to be oversight regarding implementation of any risk identification and mitigation program primarily due to pushing from one extreme to

“Combining military insider-threat training along with successful university practices, we can start to piece together a legitimate process for universities and organizations to use.”

advanced research with Stanford's students and faculty. This program brings together great minds and a tremendous opportunity for Chinese students to be embedded into a central hub for engineering and innovation within the United States. With that opportunity also comes tremendous risk for the intellectual property that comes out of the research. In reviewing the protocol for acceptance into the program, Chinese universities select the eligible individuals and prepare applications for Stanford faculty to select from. Each Stanford faculty member chooses the individual best suited for the program and the requirements. Upon acceptance, “the China Programs staff coordinates this process and, once the students are selected, organizes their admission to Stanford, visas, housing, travel, and other logistics.”<sup>15</sup> Although Stanford does not control the competitive Chinese application process, the university does control the selection and acculturation process of students. The program does not specifically outline if the research associated with the program is sensitive or not. A question we should ask in this case is: What training on intellectual property and cultural sensitivity do the faculty, staff, or students have? In order to maintain the overall intent of collaboration, Stanford staff maintains the application selection process and procedures. Combining military insider-threat

the other. For example, a 2018 *New York Times* article discussed Duke's suspicions of possible espionage involving the technological advancements of a Chinese researcher while at the university in 2008. “The researcher, who was investigated by the FBI but never charged with a crime, ultimately returned to China, became a billionaire, and opened a thriving research institute that worked on some projects related to those he studied at Duke.”<sup>16</sup> The technological advancements were directly related to creating an “invisibility cloak” that could take fighter jets off a radar system at any time. This research is now making its way through Chinese defense funding and has emerged as a potential national security issue.

Fast forward to January 2019, where the director of graduate studies in the Duke University School of Medicine's Master of Biostatistics Program was asked to step down for comments made to students about speaking only English, even within the lobby of the school, to “demonstrate a deeper commitment to their program.”<sup>17</sup> It was not the first email the director had sent regarding language use. Even though this person remains on staff, the concerns over xenophobia and racism after the incident have scarred some of the Duke community.

If universities follow best practices for inclusive programs that enrich and nourish the important ties between







Our understanding of intellectual property and the laws that govern research and development are quite different from those in China.



staff, students, and the community, it will build the loyalty and sense of belonging that is the basis for trust. Similarly, the U.S. military puts a lot of emphasis on the importance of trust; truly, our foundation is built upon trust first.

### Alternative Viewpoint

Arguments against further restrictions on access to research emerge out of the discussion surrounding information that would be accessible by anyone once it is published and distributed anyway. Another argument is that information or breakthroughs generated in research would not be possible if not for the contributions from international students. And we know that some information obtained and the professional networking that occurs during the research process goes above and beyond the expected outcome. However, these facts are irrelevant to the arguments for identification, data collection, and recruitment.

In many cases, hindsight and lessons learned are the only ways to know something had the potential to do further damage than anticipated. For example, in the case of Liu Ruopeng at Duke University, photos and information were used by China at an accelerated rate compared to that in the university setting, impacting the Chinese industry and market along with the United States. China embedded professors for the sole purpose of creating the technology first.

Duke's experience with xenophobia is not a novel occurrence. The reputation of Duke, along with similarly targeted institutions, affects their legacy and their expectations moving forward. Organizations can overreact on both sides. The solution lies with using data that can work as an advantage in regulating how universities respond to incidents. Collecting data also provides the analysis needed to know what type of education and training are necessary to reach the ideal outcome described in the *National Security Strategy*. The notion of subjecting all Chinese or international students to rigorous, or worse, xenophobic vetting, is abhorrent,

unrealistic, and a tremendous disservice to the practice and embodiment of university research.

It comes as no surprise that the information and discussions generated in universities are desired by our adversaries. Since the launch of Sputnik in the 1960s, the affiliation between government and academia has been a love-hate relationship. *Spy Schools* addresses past and even recent interworkings of the CIA and other U.S. agencies embedded within universities, known and unknown to students and faculty. This raises questions on academic boundaries, integrity, and trust between organizations. Government involvement within research is not always welcomed or wanted. However, transparency is key, and the evidence of Chinese interactions and the billion-dollar companies emerging from U.S. educated students is undeniable.

Recent news has highlighted the work of He Jiankui, a scientist who has now officially and successfully genetically altered babies in China. Although Chinese born, he gained his education from Rice University and Stanford University, where he worked with Stanford bioengineering and applied physics professor Stephen Quake, who works on DNA sequencing. He then took his knowledge and experience with sequencing DNA and built on it to alter DNA (something that gene-editing experts have feared since creating the technique coined CRISPR).<sup>18</sup> Some of the same technology is used within U.S. programs, but our understanding of intellectual property and the laws that govern research and development are quite different from those in China. These are all facts we have to consider when recruiting and accepting students who are planning to return to their home country with systems and processes gained at our country's top universities.

### Implications and a Call to Action

The use of military practices may not always translate into the higher education world. In fact, the philosophical and practical approaches to these issues are frequently in opposition. A military response often





requires extreme vetting as the most direct method to mitigate risks, whereas the core framework for higher education thrives on the power of collaboration across multiple disciplines, abilities, and cultures. However, the fundamental belief in protecting information can be capitalized and leveraged within universities with the assistance of military decision-making, problem-solving strategies, and the ideals of joint collaboration. Military partners would have to provide monitoring and report training for faculty and students that could be disseminated across sensitive programs and partnerships. The whole idea of “if you see something, say something” remains an effective means to thwart threats due to the fact that everyone has a buy-in and must contribute to keep us all safe. In *Spy Schools*, Golden notes, “It wouldn’t be that hard to tighten up the intellectual property rules and have written collaboration agreements and have more courses about intellectual safeguards.”<sup>18</sup> The ever-vigilant mentality, training, and implementation must be inclusive due to the very nature of diversity within higher education. If we force these efforts in the wrong way, we stand to lose a lot more than research and development; the core ideals of our education systems are at stake, and we can lose the students who make our programs and advancements possible.

Higher education institutions are responsible for implementing and evaluating the success of their programs and must report those findings to government partners in order to find those tricky but all too dangerous single points of failure for universities. The side effect of increased training and vigilance could increase reporting regardless of the true occurrence of actual espionage. This walks dangerously along the line with the incorrigible actions surrounding the mistreatment of students that have been reported in the past.

For higher education institutions, the adjustment to government or military involvement is also a concern. The nature of exploratory research and the spirit of academia may clash with the restrictive culture of outside interests. For the path of least resistance, and in keeping with the ideals of academic endeavors, monitoring and reporting at the student and faculty level is a possible plan of action. Much like priorities within the military, universities that have been identified as sensitive research institutions must incorporate initial and long-term plans for integration and evaluation of the lines of effort. Using similar platforms to DAPRA’s Polyplexus design, we can provide structure and potential systems to help universities tackle the depth of research exposure while encouraging advanced research and tapping into the benefits of social media and other modern forms of collaboration.

## Conclusion

The burden of success is remaining just that—successful. Our nation competes globally but rarely looks into the safeguarding of our innovations during their infancy at the academic level. Failure to protect intellectual property and the exploitation of U.S. education systems have potentially dire consequences. This article serves as a means for providing viable solutions to the potential threats and issues related to the U.S. National Security Innovation Base.<sup>20</sup> The proposed call to action regarding national security priorities must be addressed if we intend on mitigating the risks associated with allowing faculty and students to work and research autonomously (without an understanding of the infinite impact they could have on our national security, our intellectual advancement, and our economic prosperity). As Americans, we must embrace both realism and idealism so we know which “stones” are worth keeping, how to protect them, and which ones we should share. ■

## Notes

**Epigraph.** A proverb, often erroneously attributed to Confucius, the origin of which appears to be linked to the name of a Daoist parable included in the 4th Century A.D. works of Liè Yǔ Kòu, <https://www.goodreads.com/questions/1156657-what-is-the-meaning-of-the-man-who-moves>.

1. John A. Van Messel, “Unrestricted Warfare: A Chinese Doctrine for Future Warfare?” (master’s thesis, Marine Corps University, 2005).

2. Will Knight, “The Dark Secret at the Heart of AI,” *MIT Technology Review* (website), 11 April 2017, accessed 22 March 2019, <https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/>.



3. Daniel Golden, *Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities* (New York: Picador, 2018), 6.

4. David E. Sanger and Nicole Perlroth, "6 Chinese Men Indicted in Theft of Code From U.S. Tech Companies," *New York Times* (website), 19 May 2015, accessed 22 March 2019, <https://www.nytimes.com/2015/05/20/technology/6-chinese-men-indicted-in-theft-of-code-from-us-tech-companies.html>.

5. Golden, *Spy Schools*.

6. *Ibid.*, 8.

7. *Ibid.*, 13.

8. "Creating Breakthrough Technologies and Capabilities for National Security," Defense Advanced Research Projects Agency, accessed 23 March 2019, <https://www.darpa.mil/>.

9. *Ibid.*

10. The White House, *The National Security Strategy of the United States of America* (Washington, DC: The White House, 2017).

11. "How Manufacturing Incubators Are Moving Manufacturing into the 21st Century," *Goldin Peiser & Peiser* (blog), 7 December 2015, accessed 8 July 2019, <https://blog.gppcpa.com/blog/enewsletters/article/how-manufacturing-incubators-are-moving-manufacturing-into-the-21st-century>.

12. "Creating Breakthrough Technologies and Capabilities."

13. "Inspector General Reports," Oversight.gov, accessed 23 March 2019, <https://oversight.gov/reports>.

14. Golden, *Spy Schools*, 6.

15. "Chinese Undergraduate Visiting Research Program," Stanford School of Engineering, accessed 23 March 2019,

<https://engineering.stanford.edu/students-academics/programs/global-engineering-programs/chinese-ugvr>.

16. Ana Swanson and Keith Bradsher, "White House Considers Restricting Chinese Researchers over Espionage Fears," *New York Times* (website), 30 April 2018, accessed 22 March 2019, <https://www.nytimes.com/2018/04/30/us/politics/trump-china-researchers-espionage.html>.

17. Sarah Mervosh, "Duke University Apologizes over Professor's Email Asking Chinese Students to Speak English," *New York Times* (website), 27 January 2019, accessed 22 March 2019, <https://www.nytimes.com/2019/01/27/us/megan-neely-duke-chinese.html>.

18. Gina Kolata, Sui-Lee Wee, and Pam Belluck, "Chinese Scientist Claims to Use Crispr to Make First Genetically Edited Babies," *New York Times* (website), 26 November 2018, accessed 22 March 2019, <https://www.nytimes.com/2018/11/26/health/gene-editing-babies-china.html>.

19. Nick Roll, "The CIA within Academe," *Inside Higher Ed*, 3 October 2007, accessed 22 March 2019, <https://www.insidehighered.com/news/2017/10/03/spy-schools-how-cia-fbi-and-foreign-intelligence-secretly-exploit-america's>.

20. Daniel Morgan, "The New National Security Innovation Base: Charting the Course for Technology in War," *Modern War Institute at West Point*, 20 February 2018, accessed 27 June 2019, <https://mwi.usma.edu/new-national-security-innovation-base-charting-course-technology-war/>.

