NMCIWG SPECIAL REPORT

ESPIONAGE WITHIN ACADEMIA

… An Open Source History Lesson

Revision: 1b
Updated: 5 September, 2013

Contents

INTRODUCTION

U.S. based academic institutions are an *integral* and *highly valued* component of the U.S. research and development (R&D) cycle. Academia contributions towards the creation of military and dual-use technologies (i.e. military application *and* civilian use) are of *immeasurable benefit* to our country.

Faculty staff and research students that engage in R&D efforts are self-motivated to produce quantitative research that meets, or exceeds, contracted expectations. Foreign national students that possess unique skillsets are sometimes authorized to participate in the contract efforts with the expressed permission of the contract issuer. Statistically, the vast majority of research efforts are worked, from start to finish, without any loss or theft of information - however, there have been well-documented instances where "rogue actors" decide to commit acts of espionage, insider threat and/or sabotage of those efforts. Academic computer networks are frequently targeted to gain unauthorized access to protected information. Academia faculty members have been targeted due to their experience and access to sensitive information. Some of these espionage efforts are self-motivated by a disillusioned employee or student; most are well-coordinated campaigns that are conducted patiently and with purpose towards a specific data acquisition goal.

George Santayana, renowned philosopher and novelist, perhaps said it best in his published works titled "The Life of Reason"

"Those who cannot remember the past, are condemned to repeat it"

OVERVIEW

This publication seeks to educate the reader, using Open Source Intelligence (OSINT) news articles and unclassified research papers, of threats posed against the academic community from Foreign Intelligence Entities (FIE). FIE actors pose an extremely serious threat to the security of the United States; history has shown their efforts have been successful, and the damage they have inflicted is irreversible. As is true with terrorist threats, espionage does not require dozens of participants to be effective – **ONE INDIVIDUAL** that possesses harmful intentions is all that is required to inflict grave damage.

Information contained within this NMCIWG publication is purposely presented in a bulleted format (i.e. only the "meat and potatoes" is presented). The OSINT material is organized into sections to facilitate reading and self-initiated academic espionage research efforts.

The New Mexico Counterintelligence Working Group (NMCIWG) has vested interests with your facility, as most of its membership's employers have active grants and/or contracts with your campus. NMCIWG members are enthusiastically poised to provide a full suite of counterintelligence (CI) services to help your Facility Security Officer protect the sensitive materiel that has been entrusted to your institution.

We understand that groundbreaking research requires collaboration, overseas travel and publishing of materiel. We do NOT want to become an obstacle – instead, we want to become a valued ally that can provide assistance/guidance when necessary to ensure your customers receive a final deliverable product that is uncompromised – because that is what is required in today's multi-faceted threat environment to protect our country!

DEFENSE SECURITY SERVICE (DSS)

1) DSS 2013 Targeting U.S. Technologies Handbook [D]:
   a) Academic Solicitation Definition: Via requests for, or arrangement of, peer or scientific board reviews of academic papers or presentations, or requests to study or consult with faculty members, or applications for admission into academic institutions, departments, majors, or programs, as faculty members, students, fellows, or employees
   b) Academic solicitation was the top Modus Operandi used in FY12 by countries that comprise the "Near East" (e.g. Iran, Israel) – this method accounted for 49% of attempts from this region to illegally acquire U.S. missile technology
      i) Academic solicitations increased 80% between FY11 and FY12
   c) Academic solicitation that originated from countries that comprise the South and Central Asia (e.g. India, Pakistan) increased from 9% to 25% between FY11 and FY12
   d) Academic solicitation that originated from countries that comprise the East Asia and Pacific (e.g. China, Taiwan) increased 42% between FY11 and FY12
2) DSS 2011 Technology Trends handbook [E]: eightfold increase in attempts by countries in East Asia, including China, to obtain classified or proprietary information by "academic solicitation," such as requests to review academic papers or study with professors

FEDERAL BUREAU OF INVESTIGATION (FBI)

1) 2011 FBI white paper [F]
   a) Universities are an "ideal place" for foreign intelligence services
   b) Useful "to find recruits, propose and nurture ideas, learn and even steal research data, or place trainees
   c) Foreign governments pressure legitimate students to report information to intelligence officials "back home"

FEDERAL SURVEYS

1) A 2009 federal survey conducted on foreigners stateside on temporary visas [A]
   a) Made up 46% of science and engineering graduate students at Georgia Institute of Technology and Michigan State
   b) Made up 41% at Massachusetts Institute of Technology
2) Per the Institute of International Education in New York [A]
   a) China sent 76,830 graduate students to U.S. universities in 2010-2011
   b) Higher than any other country and up almost 16% from the prior year
3) Association of University Technology Managers in Deerfield, Illinois [A]
   a) U.S. and Canadian universities reaped $2.5 billion in 2011 from licensing technology, up from $222 million in 1991

U.S. EDUCATED FOREIGN INTELLIGENCE ENTITIES (Hanjuan Jin, Li Fengzhi)

1) American universities have sometimes educated Chinese researchers who later committed corporate espionage against the U.S. (A)
   a) **HANJUAN JIN** (B), a former software engineer at Motorola Inc., was found guilty in February 2012 in federal court of stealing Motorola trade secrets to benefit China's military
      i) She stole over 1000 Motorola sensitive documents
      ii) Sentenced to four years at a federal prison for stealing trade secrets
      iii) Jin joined the company, now known as Motorola Solutions Inc. (MOT), after earning a master's degree from the University of Notre Dame
      iv) While at Motorola, she received a second master's, this time in computer science, from the Illinois Institute of Technology in Chicago
   b) **LI FENGZHI**, who worked for years as a Ministry of State Security (MSS) former Chinese Intelligence Officer (Q)
      i) Defected to Canada in 2003; provided a lengthy interview that revealed the MSS mission:
         (1) MSS was patterned after the Russian KGB
         (2) "Focused on sending spies to infiltrate the U.S. intelligence community and collecting secrets and technology from the U.S."
         (3) "China spends a tremendous effort to send out spies to important countries like the U.S. to collect information"
         (4) The MSS is China's main civilian spy service. It's military counterpart, the Second Department of the People's Liberation Army, or 2PLA, is focused on stealing foreign technology, much of it for weapons and military systems
         (5) Together, the MSS and 2PLA are estimated to have several thousand trained operatives working around the world, most posing as diplomats, journalists, business representatives and academics. Thousands of other Chinese nationals also function as semiprofessional information gatherers
         (6) Fenghzi said that as a doctoral candidate, the MSS sent him to study at an American university, an experience that influenced in his decision to defect
         (7) Fengzhi was granted U.S. asylum by a Denver judge in late 2010

FIE EMPLOYER MISDIRECTION (Yu Xiaohong)

1) A foreign scientist's military background, affiliation or purpose isn't always apparent or honestly disclosed (A)
   a) Professor Daniel J. Scheeres granted a request from **YU XIAOHONG** to study with him at the University of Michigan
      i) Xiaohong expressed a "pretty general interest" in Scheeres's work on topics such as movement of celestial bodies in space
      ii) Xiaohong cited an affiliation with the Chinese Academy of Sciences, a civilian organization
      iii) The Beijing address Yu listed in the Michigan online directory is the same as the Academy of Equipment Command & Technology, where instructors train Chinese military cadets and officers
      iv) Yu co-wrote a 2004 article on improving the precision of anti-satellite weapons
      v) Once Yu arrived, her questions made him uncomfortable; as a result, he stopped accepting visiting scholars from China

vi) Per Scheeres, "It was pretty clear to me that the stuff she was interested in probably had some military satellite-orbit applications,"
vii) Yu later wrote a paper on the implications for space warfare of the NASA Deep Impact mission, which sent a spacecraft to collide with a comet

STUDY ABROAD STUDENT TARGETING (Glenn Duffie Shriver)

1) Potential targets for intelligence services (A)
   a) More than 270,000 Americans studied abroad for credit in 2009- 2010, a 4% increase from the year before.
   b) President Barack Obama has announced an initiative to send 100,000 American students to China, and China has committed 10,000 scholarships for them.
   c) As a junior at Grand Valley State University in Allendale, Michigan, GLENN DUFFIE SHRIVER studied at East China Normal University in Shanghai.
   d) After graduation, he fell into employment with Chinese intelligence agents, who paid him more than $70,000 to do their bidding
   e) At their request, he returned to the U.S. and applied for jobs in the State Department and the CIA to gain access to sensitive information on behalf of his Chinese handlers
   f) Jan 2011: sentenced to four years in prison after pleading guilty to conspiring to provide national-defense information to Chinese intelligence officers
2) "Study-abroad programs are an attractive target. Foreign security services find young, bright U.S. kids in science or politics, it's worth winning them over," (A)

FRONT COMPANIES AND FOREIGN STUDENTS

1) Front companies have been leveraged by FIE to finance/direct foreign students that are enrolled within U.S. academia (A)
   a) China's intelligence service deploys a freelance network including students, researchers and front companies
   b) China has "lots of students who either are forced to or volunteer to collect information"
   c) 'If it wanted to steal a beach, Russia sends a forklift. China sends a thousand people who would pick up a grain of sand at a time.'"
2) "Intelligencer: Journal of U.S. Intelligence Studies", fall/winter 2006-2007 edition (C)
   a) China also has more than 3,000 front companies in the U.S. "for the sole purpose of acquiring our technology"

CASE STUDIES/OPEN SOURCE REPORTING

2011 FBI REPORT (A)

1) International conference hosts invited a U.S. researcher to submit a paper. When she gave her talk at the conference, they requested a copy, hooked a thumb drive to her laptop and surreptitiously downloaded every file from the laptop
2) Asian graduate student arranged for researchers at home to visit an American university laboratory and take unauthorized photos of equipment so they could reconstruct it in their homeland

HOUSE OF REPRESENTATIVES COMMITTEE, 16 May 2013 (N)

1) Testimony of Larry M. Wortzel before the House of Representatives Committee on Science, Space and Technology Subcommittee on Investigations and Oversight. Committee focused on balancing scientific cooperation, the protection of critical information, and the espionage threat from China. Mr. Wortzel presented the U.S.-China Economic and Security Review Commission's findings on China's science and technology policy and its goals, priorities and strategies with respect to the United States
   a) The Chinese Academy of Sciences operates 100 research institutes; there are more than 45,000 other research institutes and laboratories in China
      i) This nationally directed infrastructure seeks to obtain technology from foreign firms in key scientific areas that often have military application
      ii) Many of China's researchers and scientists have trained at U.S. institutions or have worked in U.S. firms, also adding to the transfer of American technology
   b) There is a substantial espionage threat posed by the large number of Chinese nationals working at U.S. laboratories and academic institutions
   c) Three former U.S. officials, Mike McConnell, former Director of National Intelligence; Michael Chertoff, former Secretary of Homeland Security; and William Lynn, former Deputy Secretary of Defense, stated in a January 27, 2012 Wall Street Journal opinion piece:
      i) "The Chinese government has a national policy of espionage in cyberspace"
      ii) "It is more efficient for the Chinese to steal innovations and intellectual property than to incur the cost and time of creating their own."
   d) "If laboratories or academic institutions are engaged in fundamental research and at the same time are involved in research on proprietary, export-controlled or classified matters, it is incumbent on the government or industry to ensure that foreign nationals do not get unauthorized access to export controlled or classified research. Also, the information systems of institutions involved in controlled or classified research should be separate from those that are open to all researchers."

CIA/FBI 1999 Report to Congress on Chinese Espionage Efforts against the U.S. (P)

1) CIA/FBI Report to Congress on Chinese Espionage Efforts against the U.S.
   a) Authors: George Tenet (CIA Director) and Louis Freeh (FBI Director)
   b) Addressed to: J. Dennis Hastert, Speaker of the House of Representatives
2) Report highlights include:
   a) The Chinese intelligence services have a long history of using Chinese students studying abroad to collect information, either formally for those services or informally for their home-based research institutes or universities
   b) Many Chinese students in U.S. graduate schools are studying hard sciences and are able to collect a wide variety of information that is of value to China's efforts to ascend the technology ladder
   c) Some of the thousands of Chinese students, scientists, researchers, and other visitors to the United States also gather information, working mostly for the benefit of government-controlled, end-user organizations and other scientific bureaus, research institutes, and enterprises. The Ministry of State Security (MSS), when requested, assists these institutions by matching their information needs with assets the service has developed in the United States or elsewhere
   d) The primary targets from which China seeks to acquire sensitive and restricted proprietary/trade secret U.S. technology are the U.S. Government, private U.S. Corporations, academic institutes, laboratories, as well as persons involved in sensitive and/or restricted work

Unclear Boundary between Academic and Military Research

1) This open source article [R] proclaimed:
   a) Recent reports show that the line between military intelligence operations and academic research is often blurred in China
   b) According to several academic papers in the public domain, faculty members at Shanghai Jiaotong University have conducted research on cyber security along with the People's Liberation Army unit linked to hacking attacks on U.S. corporate networks in a report last month, Reuters reported
      i) The academic papers suggest that the dividing line between certain Chinese universities and the PLA is much hazier than it might be in some countries
      ii) Beijing-based academic Chen Yongmiao said the lines are far more clearly drawn in Western countries between academic research and intelligence operations than they are in China
      iii) Chen said "all of China's universities are run by the Communist Party"
      iv) Chen said "Chinese universities aren't like Western universities; they don't have the academic freedom or the independence you'd expect at a university"

OPEN SOURCE REPORTING

Chen Dingchang

Study conducted by the Project 2049 Institute located in Arlington, Virginia stated [A]

1) University of Florida was visited by **Chen Dingchang**, the head of a Chinese military-sponsored working group on anti-satellite technology, led a delegation in 1998 to the University of Florida to learn about diamond-coating manufacturing, used in missile seekers and other systems
2) In a 1999 report in a Chinese journal, the authors, including Chen, said the university's cooperation would assist in overcoming a technical bottleneck in China's development of anti-satellite warheads

J. Reece Roth

University of Tennessee Professor **J. Reece Roth** [G]

1) Plasma physics expert that utilized the campus' laboratory to conduct work on two United States Air Force contracts between 2004 and 2006
2) Roth provided sensitive export controlled research UAV plasma guidance system information to Chinese and Iran graduate students
   a. Roth took a laptop that contained export controlled data to China during a 2006 lecture tour; an additional sensitive report was sent to Roth via e-mail via a Chinese professor's Internet connection
3) Roth pled guilty to 10 counts of exporting defense-related materials
   a. Found guilty conspiracy, wire fraud and 15 counts of exporting defense articles and services without a license
   b. Sentenced to four years in prison

Yin Qingqiang

Cornell University postdoctoral research associate **YIN QINGQIANG** [G]

1) Was actively involved in phytase enzyme research funded via government grant

2) A Chinese research facility offered YIN a job located in China in exchange for materials that could be used to copy phytase
3) YIN was arrested in an airport security checkpoint with more than 100 glass vials and containers of material that belonged to the university
4) YIN was charged with conspiracy to defraud the U.S. government and received 12 months in prison

Lidiya Guryeva

Columbia University master degree program student **LIDIYA GURYEVA** [(H)(I)]

1) Used the cover name of "Cynthia Murphy" – she was, in reality, a Russian intelligence officer that participated in the Russian sleeper agents program that involved 12 undercover spies (including Anna Chapman)
2) Instructed by Russian intelligence to "strengthen ties with classmates and professors on a daily basis who could help her in "job search and have, or will have, access to secret information"
3) Graduated from New York University and Columbia Business School
4) Attempted to build a close relationship with a venture capitalist who co-chaired Hillary Clinton's 2008 presidential bid
5) Pleaded guilty on charges of failing to register as a representative of a foreign government and then exchanged to the Russian government

Jose Cohen Valdes

Cuban Intelligence Officer **JOSE COHEN VALDES** documented Cuban penetration into U.S. academia [(J)]

1) Cuba learned the value of penetrating U.S. academia from Russian intelligence
2) As of 2009, the Cuban regime considered the penetration infiltration of U.S. academia as a top priority – they seek out students who might ultimately occupy positions of importance in the private and government sectors
3) Cuban intelligence study and analyze all accessible information about U.S. universities
    a. Political and social tendencies of professors and students
    b. Programs of study and individual studies
    c. Valdes' report specifically mentioned these institutions: Harvard University, Yale University, New York University, Hunter College, Columbia University, American University, Georgetown University, the University of Pennsylvania, University of California at Berkeley, and Massachusetts Institute of Technology (MIT)

Timo Kivimaki

Professor **TIMO KIVIMAKI,** political science department, Copenhagen University [(K)]

1) Between 2002 and 2012, Kivimaki visited the Russian embassy 20 times
2) During the meetings, Kivimaki was paid to reveal university personnel who had the potential to attend scientific seminars and could be invited to perform research on specific themes
3) Sentenced to 2.5 years home arrest

Hua Jun Zhao

Medical College of Wisconsin employee **HUO JUN ZHAO** [(L)]

1) Three vials of a possible cancer-fighting compound disappeared recently from a professor's desk

2) Security video showed ZHAO as the only person who entered the professor's office that day
3) Investigators found 384 files related to Anderson's research, as well as research results from another professor from the school's cancer department
    a. Among the files was a grant application to a Chinese foundation that Zhao wrote in Mandarin
    b. In the application he said he discovered the C-25 compound and that he was seeking funding to continue his research in China
4) Allegedly took steps to provide that material to Zhejiang University in China
5) The stolen vials of the C-25 powder are worth $8,000
6) ZHAO's co-workers told the FBI that Zhao spoke excellent English and he had lived in the U.S. for many years
7) ZHAO is charged with economic espionage, which carries a maximum penalty of 15 years in prison and a $500,000 fine
8) ZHAO traveled to China in December 2012
9) School security staff told FBI agents that on the day of his suspension Zhao also accessed school computers remotely and deleted files related to the C-25 research
10) Federal authorities subsequently searched Zhao's home and found a receipt for shipment of a package to Zhao's wife along with two airline tickets from Chicago to China leaving Tuesday, as well as an application to the National Natural Science Foundation of China for research funding for C-25

The Cambridge Spy Ring

The **CAMBRIDGE SPY RING** (K)

1) During the 1930s numerous young men that attended Cambridge University were successfully recruited by the KGB to spy on behalf of Russia
2) Five students agreed to spy for Russia – their motivation was the belief that capitalism was corrupt and that the Russian model for society was superior
3) **KIM PHILBY**, **GUY BURGESS**, **DONALD MACLEAN**, **ANTHONY BLUNT** and **JOHN CAIRNCROSS** where the five spies that comprised the Cambridge Spy Ring
4) **PHILBY** later worked for British Intelligence, secretary of the British embassy in Washington, the CIA, and as a journalist in Beirut. He disappeared in 1963, but it was later discovered he had moved to Russia and had been granted Russian citizenship
5) **BURGESS** worked at the BBC, MI5 and eventually worked with PHILBY at the embassy. He disappeared in 1950, only to emerge in Russia and eventually died in Russia
6) **MACLEAN** joined the diplomatic service and in 1950 became head of the American Department at the Foreign Office where he had access to Top Secret atomic development information. He left for Russia with BURGESS when he learned he was under suspicion. It was later discovered he helped fellow spy **BLUNT** escape to Russia
7) **BLUNT:** Acted as a talent scout that supplied names of possible recruits that would support the communist cause. During WWII he worked for British Intelligence. In 1964 **BLUNT** exchanged immunity for his confession for his involvement with the Cambridge Spy Ring. In 1979 he was stripped of his knighthood and academic honors
8) **CAIRNCROSS** was recruited to the Communist Party in 1937 and worked in the Foreign Office alongside **MACLEAN**. During his Treasury employment he leaked details about a military decoding center (Bletchley Park) – that information enabled Soviet spies to change their encryption codes to

mitigate British decryption efforts. Information that **CAIRNCROSS** provided on American and British atomic weapon programs are thought to be the foundation of the Russian nuclear program

Jiangyu Zhu and Kayoko Kimbara

Harvard Medical School postdoctoral research fellows **JIANGYU ZHU** and **KAYOKO KIMBARA** (O)

1) Admitted to stealing materials from Professor of Cell Biology Frank D. McKeon's lab at Harvard Medical School in December, 1999, when both were preparing to leave Harvard for the University of Texas at San Antonio, TX
2) They shipped more than 20 boxes of sensitive medical materials to Texas, where they were recovered in June, 2000
3) The stolen materials were crucial to research involving calcineurin, an enzyme that causes the immune system to reject transplanted organs
4) Immediately before leaving Harvard, Zhu and Kimbara had found genes that block calcineurin—a lucrative discovery for drug development
5) Both had signed Participation Agreements agreeing that all of their discoveries and materials belonged to Harvard

Yudong Zhu, Xing Yang, and Ye Li

1) **YUDONG ZHU, XING YANG,** and **YE LI** (S) were three MRI technology researchers working at a university located in NY, NY
2) All three individuals had undisclosed affiliations with a Chinese company performing the same type of research
3) On 20 May 2013, the defendants were each charged with one count of commercial bribery in connection with a conspiracy to receive payments from the Chinese company and a Chinese government-supported research institution in exchange for providing non-public information about research they conducted at the university
4) Zhu is also charged with lying about conflicts of interest in connection with the federal research grant
5) Zhu and Yang were arrested at their residences in New York yesterday, and Li is believed to have flown to China before charges were brought against Li
6) In 2008, the NY-based University hired Zhu, an accomplished MRI researcher and innovator, to teach and conduct research related to innovations in MRI technology. Zhu came to the university, in large part, to use a specific university laboratory that possessed highly specialized equipment to test MRI innovations
7) In 2010, Zhu caused the university to apply for and receive a grant from the National Institutes of Health (NIH) that provided millions of dollars in funding over a five-year period for Zhu's research relating to improving the imaging capability of MRI equipment (the "NIH grant"). After Zhu started his research pursuant to the NIH grant, he arranged for Yang and Li to move to New York from China to work with him in 2011 and 2012, respectively
8) While working for the University, Zhu, Yang, and Li each had undisclosed affiliations with a Chinese-based medical imaging company and a Chinese-government sponsored research institute
9) Zhu arranged for Yang and Li to receive certain financial benefits from a co-conspirator that was an executive with the imaging. For example, Zhu arranged for the Chinese executive to pay for Yang's tuition at a graduate school in New York, New York, that was affiliated with the university

and Li's rental apartment. The Chinese executive also paid for Yang and Li's travel between China and New York while they worked at the university

10) Yang admitted to sharing university research results with the Chinese imaging company between Aug 2011 and Jan 2013; the sensitive information included MRI equipment prototypes, experiments, and project updates. These e-mails were sent to and/or from accounts including Zhu's personal Gmail account, his United Imaging e-mail address, and Yang's Hotmail account

Terfenol-D Theft by PRC Students from Iowa State and Pennsylvania State

1) In 2003, the FBI alleged that two Chinese students (one attended **Iowa State University**; the other attended **Pennsylvania State University**) stole sensitive information from Ames Laboratory (located on the Iowa State University campus) via computer hacking
2) The stolen information pertained to a "smart material" known as Terfenol-D; originally developed under U.S. Navy contract by Ames Lab in the 1970s, the Pentagon classifies Terfenol-D as a material that is used in "militarily critical naval and aerospace applications". In 2003, Congress appropriated over $5 million for continued research on the material
3) The U.S. Navy uses Terfenol-D in advanced sonar systems for tracking enemy submarines. Terfenol-D is an export controlled technology
4) One of the students attended Iowa State and was said to have worked closely with the Ames Lab. One of the two students admitted supplying the Chinese military with the Terfenol-D data
5) The FBI cites this as a good example of how the Chinese are acquiring dual-use military technologies in the United States. In an interview with the Associated Press, a senior FBI official charged that many of the thousands of Chinese visitors, students, and businessmen come to the United States each year with tasking from Beijing to collect intelligence information
6) The Pentagon report labeled academic exchanges as one of the prime methods the Chinese use to collect sensitive technologies, like Terfenol-D. The report also said the authoritative Chinese journals have recommended an increase in the use of overseas ethnic Chinese scientists to acquire foreign technologies.

Marta Rita Velazquez

MARTA RITA VELAZQUEZ (T) graduated Princeton in 1979 and then Georgetown University Law Center in 1982

1) She allegedly recruited Cuban spy Ana Belen Montes when the two were students at the John Hopkins University School of Advanced International Studies (where Velazquez obtained a master's degree in 1984)
2) Velazquez went on to work as an attorney adviser at the U.S. Department of Transportation and as a legal officer with the State Department's U.S. Agency for International Development, where she held a top secret security clearance
3) The February 2004 indictment claims Velazquez helped Montes obtain work as a Defense Department analyst
4) In 2002, Montes pleaded guilty for conspiracy to commit espionage; she was convicted for providing classified information to the Cuban government. Montes is serving a 25 year prison sentence
5) Velazquez has lived outside the U.S. since 2002; she lives in Sweden, which does not recognize extradition requests from the U.S. for espionage allegations

Wu Chang-yu

WU CHANG-YU [U], Political Science Professor at Central Police University, Taiwan

1) Detained by police for allegations that Chinese officials offered Chang-Yu business opportunities in exchange for spying on Taiwan activities of selected Chinese persons
2) Authorities believe Chinese intelligence officers approached Chang-Yu during one of his frequent visits to China

Joel Barr

JOEL BARR [V] was an electronics engineer discovered to have committed acts of espionage against the U.S. after his defection to the Czech Republic in 1950 and then later moved to Russia

1) Barr was suspected of passing secrets to Russia; fearing arrest by the FBI Barr defected with another American electronics engineer (Alfred Sarant) – both men are believed instrumental in the development of the Russia's entire microelectronics and computer industry
2) During Barr's engineering studies at the City College of New York, Barr became friends with Julius Rosenberg and Morton Sobell. Sobell was sentenced to a 30 year prison term for conspiracy to commit espionage against the U.S. Rosenberg and his wife Ethel were sentenced to death for passing atomic weapon secrets to Russia and were executed by electric chair
3) Intelligence documents showed that Barr participated in the Rosenberg's spy ring; Barr and Rosenberg provided Russia 17 documents related to high-resolution airborne laser radar systems developed at M.I.T. and then built by Bell Labs
4) Intelligence documents stated that Barr was "among the KGB's most valuable technical spies"
5) During WWII, Barr worked in the Army Signal Corps laboratories and moved on to positions within Western Electric and Sperry Gyroscope. Those jobs provided him access to classified research and to copy classified documents about those technological advances
6) Barr provided those cloned classified documents to Rosenberg, who forwarded them to Russia
7) In 1948, Sperry Gyroscope fired Barr after discovering he was a Communist

Enos Wicher

ENOS WICHER was married to Maria Wicher and was the stepfather of Flora Wovschin

1) He was a professor at Columbia University
2) Wicher worked in the Wave Propagation Group at Columbia's Division of War Research and spied for Soviet intelligence (KGB) during WWII
3) All three, Wicher, his wife, and daughter Flora Wovshin spied for the KGB
4) His code name in Soviet intelligence and in the Venona project is "Kin" (also "Keen")
5) The Venona project intercepted codes passed among agents of the communist Soviet Union during World War II, and attempted to decrypt them. This was a project by the United States and United Kingdom during the Cold War

Byron Darling

BYRON DARLING received a Ph.D in physics from University of Wisconsin in 1939 - his specialty was in sub-atomic physics

1) He worked as a research physicist at the United Rubber Company from 1941-46 and in 1944 he was a consultant to the U.S. Office of Scientific Research & Development where he worked on various wartime projects
2) In 1953 Darling was fired from his post as associate professor of physics at Ohio State University when he refused to answer questions about Communist Party of the United States (CPUSA) ties. At that time Darling was working on a U.S. Air Force research project
3) Darling is believed to have been conducting scientific espionage on behalf of the KGB during WWII and provided Russia with atomic bomb research. Darling was a member of a group of Soviet spies led by Alexander and Helen Koral - the Koral's confessed to the FBI of being couriers for the KGB from 1939 to 1945
4) Darling participated in the WWII era Venona decryption project (as did Joel Barr)

Ryonosuke Seita

Professor **RYONOSUKE SEITA** [Z] arrived in Syndey, Australia on 14 Mar 1938 from Japan

1) Australian counterintelligence officers began monitoring Seita shortly after his arrival
2) Seita had previously been a senior diplomat in Germany and was often observed in the company of known Japanese espionage agents. Seita would later become involved in the distribution of pro-Axis propaganda leaflets in his community
3) Seita was appointed Professor of Japanese at the University of Queensland in Brisbane in 1938 by agreement between the Queensland and Japanese Governments. Seita was nominated for the position by the Japanese Foreign Office, which was heavily involved in espionage operations - Seita was now a highly placed and very influential Japanese secret agent within Australia's academic community
4) In a lecture at the Queensland University in November 1938, Seita gave a short resume of his version of Japanese policy regarding China and Japan's growing desire for expansion and power. Throughout his lecture he conveyed the impression that he admired Germany and coupled its name with Japan, as young nations who one day might challenge Britain's supremacy
5) A student of Seita's stated that Seita was pro German; that Seita had stated "Britain should return all of the German colonies otherwise she deserves what she is getting". The student also stated that Seita intended to retire in Germany. Prior to a trip to Japan, the student was given a letter of introduction to the Japanese Intelligence Department by Seita, who seemed disappointed when he discovered that the student did not utilize the letter during his visit to Japan
6) A Japanese company in Sydney paid Seita for his espionage work. Unbelievably Seita was later appointed as translator in the high security Brisbane Censor's Office from some time in 1940 until the outbreak of war. This gave Seita access to every Japanese communication in and out of Queensland. Despite pleas to remove Seita from this role, the bureaucracy would not believe that he could possibly be a Japanese Secret Agent. On 10 January 1941 Officials in Canberra had been warned that Seita was working in the Censorship Staff in Brisbane and was a security risk
7) After the Japanese attack on Pearl Harbor on 7 December 1941, Seita was arrested in Brisbane as an alien on 8 December 1941 and Australian security agents searched Seita's house. A visiting

card of Mitsuru Toyama was found in his residence. Mitsuru Toyama was the head of the feared Black Dragon Society

8) More than a year after Seita's arrest, a Brisbane Security Agency issued a secret report which confirmed that Seita was a Japanese intelligence agent. The Japanese Foreign Office later tried to arrange an exchange of Seita for several Australian internees being held in Japan. Australian Intelligence directed that Seita be held in Australia. Unfortunately their request was ignored and Seita was repatriated to Japan in August 1942.

FBI INITIATIVES

1) National Security Higher Education Advisory Board [(A)]
   a) Established by the FBI and CIA in 2005
   b) Educates academia about foreign threats posed against their campuses

NMCIWG RECOMMENDED THREAT MITIGATION STRATEGIES

CYBER THREAT

1) If wireless networks are used within the campus, ensure they require a password to access that network resource
2) Guests/visitors are not allowed to use campus owned Automated Information Systems (AIS)
3) Ensure every campus-owned AIS has active anti-virus software that scans all files stored on all attached media (internal; USB; Firewire); it's signature files are updated at least daily
4) Ensure every campus-owned AIS is current on all software patches
5) All campus-owned AIS has active encryption used on its internal storage devices
6) Rename or deactivate default Windows accounts (e.g. GUEST)
7) Ensure network infrastructure equipment (e.g. routers; firewalls) have their factory-set username/password accounts renamed
8) Create/enforce a network logon banner that informs the resource user of their expectation of privacy/punishment for hacking campus owned equipment
9) Tether campus-owned AIS using Kensington locks to immovable devices
10) Ensure campus rooms that store campus network equipment are secured at all times
11) Purchase/deploy XEROX machines do not possess internal hard drives
    a. Legacy devices with internal hard drives require the internal hard drive to be degaussed prior to their campus departure to protect stored data
12) Ensure campus network printers have current BIOS/software patches
13) Configure campus AIS wireless broadcast names that are lengthy/alphanumeric
14) Use WPA-2 encryption on campus-owned wireless networks
15) Conduct recurring inventories of campus-owned AIS equipment
16) Consider installing 'beaconing software' on campus owned AIS equipment that, when connected to the Internet, can be used to pinpoint its location

INFORMATION SECURITY THREAT

1) Ensure all contractual/proprietary/U.S. Government (Controlled Unclassified Information/For Official Use Only) is stored on a network domain that is separate from the student populace
2) Attach cover sheets on hardcopy documents that contain contractual/proprietary/U.S. government information
3) Ensure that contractual/proprietary/U.S. Government (Controlled Unclassified Information/For Official Use Only) is not accessible to students, guests and/or visitors that do not possess a valid need-to-know and/or a security clearance
4) Ensure that all campus AIS users understand the need to immediately detach a campus-owned AIS from the campus computer network should it show signs of being infected with malware
5) Ensure that all campus AIS users are trained to identify phishing/spear phishing emails; understand to NOT click on embedded hyperlinks contained within the email body/open suspicious email file attachments. The individual is NOT to delete/forward the suspicious email to another campus network email account until they have received direction from the campus Facility Security Officer
6) The Facility Security Officer can assist faculty members with campus-affiliated web site information content to ensure their biography information doesn't reveal the employee's Personally Identifiable Information or could aid social engineering efforts against the employee

7) Segregate contractual data on campus-owned AIS network servers – not only does this add an additional layer of protection from unauthorized access but also ensures the campus is able to efficiently comply with DD Form 254 requirements to surrender/destroy that contracted data upon contract expiration

PERSONNEL SECURITY THREAT

1) Ensure that senior campus faculty members; faculty that travels overseas; faculty that maintains an active security clearance notify the campus Facility Security Officer to schedule a defensive foreign travel briefing
2) Ensure that campus faculty members are briefed on elicitation/social engineering risks associated attending conferences and symposiums; the Facility Security Officer can obtain/provide them with tailored defensive briefings and arrange a debriefing should the attendee believe they were elicited

PHYSICAL SECURITY THREAT

1) Ensure all campus guests/visitors wear a lapel badge that clearly identifies them as a guest/visitor at all times while they are on the campus
2) If your facility possesses a badging system on all campus buildings, ensure that guest/visitor badges cannot open their doors. Temporary badges should not be given automatic 24/7/365 access to the facility.
3) Ensure campus faculty members know to secure all doors/windows prior to vacating a campus office
4) Ensure campus faculty members understand if they believe a campus office has been broken into that they are to NOT enter the office – instead, they notify campus security and the campus Facility Security Officer. This protects them (should the intruder still be within the office) and evidentiary material (e.g. fingerprints)
5) Ensure that campus foreign national visitors are escorted at all times while physically located on the campus. Ensure the visitor escorts receive a defensive threat briefing (via the campus Facility Security Officer) to learn of common methods used by visitors to evade their escorts/gain unauthorized access to facilities/AIS equipment and deflecting social engineering ploys

CITATIONS

ID	TITLE	PUBLISHED	INTERNET URL	ACCESSED
(A)	American Universities Infected by Foreign Spies Detected by FBI	8 Apr 2012	http://www.bloomberg.com/news/2012-04-08/american-universities-infected-by-foreign-spies-detected-by-fbi.html	22 Aug 2013
(B)	Hanjuan Jin, Former Motorola Worker, Gets 4 Years For Trade Secrets Theft	29 Aug 2012	http://www.huffingtonpost.com/2012/08/29/hanjuan-jin-motorola_n_1840833.html	23 Aug 2013
(C)	"Intelligencer: Journal of U.S. Intelligence Studies", fall/winter 2006-2007 edition	2007	Not Applicable	22 Aug 2013
(D)	Defense Security Service "Targeting U.S. Technologies" handbook, 2013 edition	2013	Not Applicable	26 Aug 2013
(E)	Defense Security Service " Technology Trend handbook, 2011 edition	2011	Not Applicable	22 Aug 2013
(F)	Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education	2013	http://www.fbi.gov/about-us/investigate/counterintelligence/higher-education-and-national-security	26 Aug 2013
(G)	Scientist arrested over trade espionage	20 Aug 2002	http://www.timeshighereducation.co.uk/news/scientist-arrested-over-trade-espionage/171296.article	26 Aug 2013
(H)	Foreign Spies Target U.S. Universities as FBI Seeks Campus Help	5 Apr 2012	http://www.bloomberg.com/slideshow/2012-04-05/foreign-spies-target-u-s-universities-as-fbi-seeks-campus-help.html#slide3	26 Aug 2013
(I)	Suspected Russian Spy Earned Degrees at Columbia, NYU	30 June 2010	http://www.dnainfo.com/new-york/20100630/manhattan/suspected-russian-spy-earned-degrees-at-columbia-nyu	26 Aug 2013
(J)	Spy universities: Ex-foreign espionage operative reveals how professors, students, and others, are recruited to undermine America	10 June 2009	http://www.inatoday.com/spyuniversities6909.htm	27 Aug 2013
(K)	Academic charged with 'spying' for the Russians	18 Apr 2012	http://www.universityworldnews.com/article.php?story=20120416204123657	27 Aug 2013
(L)	Prosecutor: Huajun Zhao, Medical College of Wisconsin Researcher, Stole Cancer Data For China	2 Apr 2013	http://www.huffingtonpost.com/2013/04/02/huajun-zhao-china-cancer_n_2998777.html	27 Aug 2013
(M)	The Cambridge spy ring	13 Sep 1999	http://news.bbc.co.uk/2/hi/special_report/1999/09/99/britain_betrayed/444058.stm	27 Aug 2013
(N)	"Espionage Threats at Federal Laboratories: Balancing Scientific Cooperation while Protecting Critical Information"	16 May, 2013	http://www.fiercegovernment.com/story/economic-espionage-threatens-openness-science-and-technology/2013-05-20	4 Sep 2013
(O)	HMS Fellows Indicted For Alleged Lab Theft	27 Jun 2005	http://www.thecrimson.com/article/2005/6/27/hms-fellows-indicted-for-alleged-lab/	4 Sep 2013
(P)	CIA/FBI Report to Congress on Chinese Espionage Efforts Against the U.S.	12 Dec 1999	http://www.fas.org/irp/threat/fis/prc_1999.html	4 Sep 2013
(Q)	Chinese spy who defected tells all	19 Mar 2009	http://www.washingtontimes.com/news/2009/mar/19/exclusive-chinese-spy-who-defected-tells-all/?page=all	4 Sep 2013
(R)	Unclear Boundary Between Academic and Military Research	26 Mar 2013	http://www.rfa.org/english/news/china/cybersecurity-03262013174440.html	4 Sep 2013
(S)	Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce Criminal Complaint Against Three New York-Based University Researchers for Conspiring to Receive Bribes from a Chinese Company and a Chinese Government-Supported Research Institute	20 May 2013	http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-criminal-complaint-against-three-new-york-based-university-researchers-for-conspiring-to-receive-bribes-from-a-chinese-company-and-a-chinese-government-supported-research-institute	5 Sep 2013
(T)	China Targets Another Energy Lab	29 Aug 2003	http://www.aim.org/media-monitor/china-targets-	5 Sep 2013

			another-energy-lab/	
(U)	Law grad's espionage indictment revealed; treaty thwarts extradition	26 Apr 2013	http://www.abajournal.com/news/article/law_grads_espionage_indictment_revealed_treaty_thwarts_extradition/	5 Sep 2013
(V)	Taiwan: Professor Wu Chang-yu Detained For Spying For China	29 Sep 2011	http://www.huffingtonpost.com/2011/09/29/taiwan-professor-china-spy_n_988246.html	5 Sep 2013
(W)	Joel Barr, Defector Linked to Rosenbergs, Dies	16 Aug 1998	http://www.nytimes.com/1998/08/16/world/joel-barr-defector-linked-to-rosenbergs-dies.html	5 Sep 2013
(X)	Entry: Enos Wicher	17 Dec 2011	http://www.conservapedia.com/Enos_Wicher	5 Sep 2013
(Y)	Entry: Byron Darling	16 Apr 2013	http://conservapedia.com/Byron_Darling	5 Sep 2013
(Z)	Japanese Master Spy in Queensland: Professor Ryonosuke Seita	15 Apr 2002	http://www.ozatwar.com/sigint/japagentseita.htm	5 Sep 2013

NEW MEXICO COUNTERINTELLIGENCE WORKING GROUP (NMCIWG)

The New Mexico Counterintelligence Working Group is comprised of counterintelligence analysts/officers, cyber experts and security professionals from these agencies: 902nd MI (Army); Air Force Office of Special Investigations (AFOSI); Defense Criminal Investigative Service (DCIS); Department of Energy (DOE); Defense Security Service (DSS); Defense Threat Reduction Agency (DTRA); Federal Bureau of Investigation (FBI); Homeland Security Investigations (HSI); Immigrations and Customs Enforcement (ICE); Los Alamos Laboratories; Missile Defense Agency (MDA); National Assessment Group (NAG); Naval Criminal Investigative Service (NCIS); Sandia Laboratories and the U.S. Attorney's office.

The NMCIWG's charter is to leverage working group participant's expertise and resources to protect cleared defense company proprietary information and Department of Defense critical program information from unauthorized compromise or theft. The NMCIWG creates/distributes a daily cyber threat newsletter and a weekly espionage threat newsletter to all New Mexico cleared company Facility Security Officers. The NMCIWG creates/distributes information bulletins and threat bulletins to all New Mexico cleared company Facility Security Officers on an as-needed basis. The NMCIWG creates/provides defensive briefings to cleared defense company employees upon request.

Purple Arrow was created in 2008 as subset of the NMCIWG – its singular focus is providing tailored multi-disciplined support to cleared defense companies located in New Mexico to protect sensitive/classified Department of Defense and indigenously-developed proprietary technologies that reside within these facilities.

To obtain additional information regarding the NMCIWG or Purple Arrow please contact SA Jeanette Greene at phone number (505) 889-1387.