

FEDERAL BUREAU OF INVESTIGATION

BALTIMORE FIELD OFFICE

FOREIGN THREATS BRIEF



COUNTERINTELLIGENCE THREATS

- Intellectual Property Theft
- Theft of Classified Information
- Economic Espionage
- Espionage
- Cyber Threats
- Insider Threats

MAJOR ACTORS

- RUSSIA



- CHINA



WAYS FOREIGN ACTORS ARE THREATS

(TO NAME A FEW...)

- **Intelligence Officers**
- **Illegals**
- **Non-Official Cover Officers**
- **Cyber Actions / Cyber Intrusions / Phishing**
- **Insider Threats**
- **Academic Threats**

RUSSIA

- Use Intelligence Officers, Non-Official Cover Officers, and Illegals to spot and assess targets of interest, recruit, steal, and spy to collect on:
 - Political Intelligence
 - Military Intelligence
 - Science and Technology
- Use economics and available funding (Russian Government) to purchase companies or majority stock in companies they want information from or use the companies to access people and information as a cover.

CHINA

- Use Non-Official Cover Officers, Academics, American citizens from China, U.S. companies owned by China /Chinese to identify targets of interest, collect / steal / buy information, and transfer the information back to China to:
 - Reduce or eliminate Research and Development
 - To advance China
 - To put U.S. companies out of business if they are or were competitors
 - Thousand Talents Program (Communist Party)
 - Academics
- China is interested in taking **ANYTHING**, from **ANY** industry.
 - Space
 - Telecommunications
 - IT, AI, ANY Technology
 - Military
 - Agriculture
 - All 16 sectors of America's Critical Infrastructure

FOREIGN THREATS INSIDE THE U. S. YOU ARE PROBABLY AWARE OF

- Six German saboteurs were executed in Washington DC for coming into the US to sabotage critical infrastructure (1942)



- Julius and Ethel Rosenberg: Spies for Russia, Manhattan Project (1953)



- Aldrich Ames, CIA (1985-1994)



- Robert Hanssen, FBI (1983 – 2001)



DID YOU KNOW ABOUT THESE NOT SO WELL KNOWN FBI CASES?

- John Walker, Jr.
- Larry Wu-tai Chin
- Jack Barsky
- Chi Mak
- Greg Chung
- Ghost Stories
- Purple Maze
- Chinese military cyber attack on Equifax in 2017
- Cyber Attacks: Colonial Pipeline

JOHN ANTHONY WALKER, JR.

- U.S. government job: U.S. Navy Warrant Officer and communications specialist, 1967 to 1985.
- Also worked for: The Soviet Union.
- Secrets passed: For more than 17 years, Walker provided top cryptographic secrets to the Soviets, compromising at least one million classified messages. After retiring from the Navy, he also recruited three people with security clearances into his espionage ring: his brother Arthur, his son Michael, and his good friend Jerry Whitworth. The information passed by Walker and his confederates would have been devastating to the U.S. had the nation gone to war with the Soviets.
- How discovered: A tip from his ex-wife.
- Fate: Arrested on May 20, 1985, pled guilty, and sentenced to life in prison.



LARRY WU-TAI CHIN



- U.S. government job: Chinese language translator/intelligence officer for CIA, 1952 to 1981.
- Also worked for: China.
- Secrets passed: Classified documents and photographs, including CIA reports on the Far East.
- How discovered: Not revealed.
- Fate: Arrested on November 22, 1985; convicted at trial but committed suicide before sentencing.

JACK BARSKY



- True name: Albrecht Dittrich, East German
- Russian Illegal; Canadian by documentation (William Dyson); Became a U.S. citizen.
- Job: Director of Software Technologies, New York Independent System Operator, NY Electric Grid Operator
- Also worked for: Russia
- Secrets passed: Classified (1978-1988)
- How discovered: Not revealed.
- Fate: Not charged because he cooperated with the FBI.

CHI MAK



- Naturalized U.S. Citizen originally from China
- Job: Engineer with defense contractor Power Paragon, part of L3 Communications.
- Also worked for: China.
- Secrets passed: Found guilty of conspiring to export sensitive defense technology.
- How discovered: Not revealed.
- Fate: Found guilty in 2007. Sentenced to 24 years in prison.

DONGFAN “GREG” CHUNG

- Naturalized U.S. Citizen originally from China
- Job: Engineer with Boeing.
- Also worked for: China.
- Secrets passed: Found guilty of stealing aerospace secrets for China between 1983 and 2006.
- How discovered: Not revealed.
- Fate: Found guilty in 2010. Sentenced to 15 years in prison.





DO YOU RECOGNIZE THIS COUPLE?
DID YOU KNOW THIS SERIES WAS TAKEN FROM A TRUE
STORY?

MICHAEL ZOTTOLI PATRICIA MILLS



- Real Names: Mikhail Kutsik and Nataliya Pereverzeva
- Came into the U.S. as Canadian citizens, changed names to dead doubles. Lived in Seattle, Washington, both attending the University of Washington where they earned degrees in business. They had two young children and then moved to Arlington, Virginia, where they were arrested.
- Job: Accountant with Sunrise Assisted Living
- Also worked for: Russia
- How discovered: Not revealed
- Fate: Arrested in 2010 (with 8 others) and traded on an airstrip in Vienna for prisoners of interest in Russia.



RELEASED BY UNITED STATES

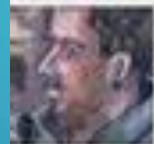
Agent's name
Real name



Richard Murphy
Vladimir Guryev



Cynthia Murphy
Lydia Guryev



Donald Howard Heathfield
Andrey Bezrukov



Tracey Lee Ann Foley
Elena Vavilova



Michael Zottoli
Mikhail Kutsik



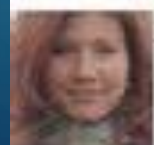
Patricia Mills
Natalia Pereverzeva



Juan Lazaro
Mikhail Vasenkov



Vicky Pelaez
Used own name



Anna Chapman
Used own name



Mikhail Semenko
Used own name

Christopher Metsos slipped bail in Cyprus

RELEASED BY RUSSIA



Igor Sutyagin
Nuclear scientist
jailed in 2004



Sergei Skripal
Military intelligence
officer convicted of
spying for UK 2006



Alexander Zaporozhsky
Jailed for espionage in 2003



Gennady Vasilenko
Former KGB officer



TRADED ON AN AIRSTRIP IN VIENNA



PURPLE MAZE

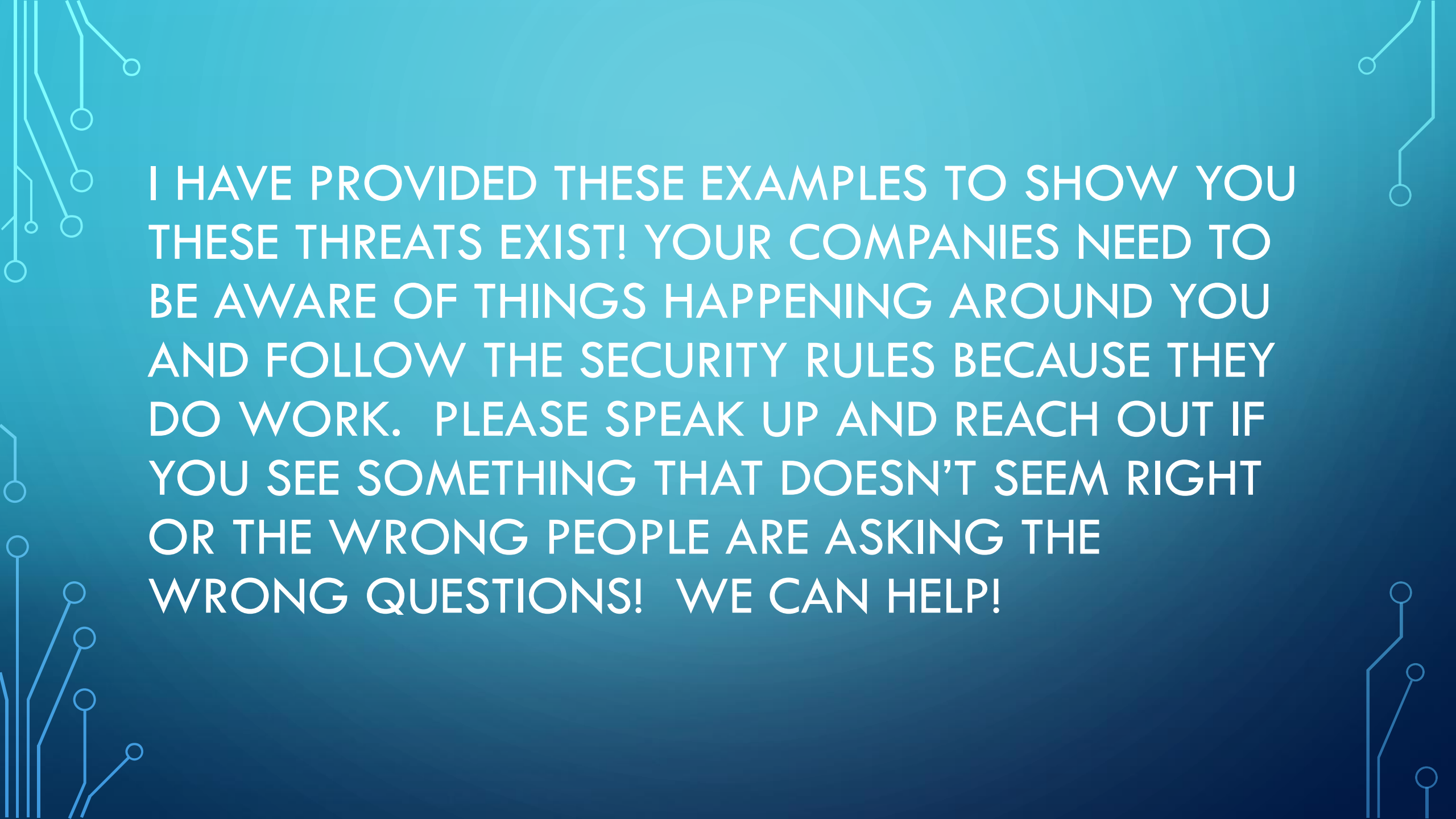
- The FBI's Purple Maze case highlights the breadth of our trade secrets and intellectual property that our foreign adversaries are trying to steal. The investigation began after Dupont Pioneer reported to the FBI a suspicious incident in one of their proprietary corn fields. What ensued was nearly a three year investigation involving wiretaps on phones, bugs in cars, and executives from one of China's largest agricultural companies attempting to smuggle corn seed out to China and Canada in microwave popcorn boxes and subway napkins hidden in their clothing. The main actor, Robert Mo (Hailong), a U.S. company owner, hosted multiple Chinese citizens and all were charged with conspiracy and theft of trade secrets / intellectual property.

CHINESE CYBERATTACK

- Four members of the Chinese military were charged in February 2020 with allegedly hacking the credit bureau Equifax (in 2017) and stealing the personal information of around 145 million Americans.
- In an indictment handed up by a grand jury in Atlanta, the men face nine counts including conspiracy to commit computer fraud and conspiracy to commit economic espionage.

COLONIAL PIPELINE RANSOMWARE ATTACK

- **Vulnerability:** Colonial Pipeline OT (industrial control systems) were available and hacked from Eastern Europe
- **Responsible:** Company named DarkSide - Ties to Russia
- Would have required Vladimir Putin's approval to go forward.
- **Ransom paid:** \$5 Million
- **Economic Impact:** Unknown
- **Effect:** Stopped the transportation of gasoline up and down the East Coast
- **Affected everyone in some way within days!**
- **Can it happen again?** Of course...and does happen all the time!

The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines and small circles, resembling electronic components or data paths. The text is centered in a bold, white, sans-serif font.

I HAVE PROVIDED THESE EXAMPLES TO SHOW YOU THESE THREATS EXIST! YOUR COMPANIES NEED TO BE AWARE OF THINGS HAPPENING AROUND YOU AND FOLLOW THE SECURITY RULES BECAUSE THEY DO WORK. PLEASE SPEAK UP AND REACH OUT IF YOU SEE SOMETHING THAT DOESN'T SEEM RIGHT OR THE WRONG PEOPLE ARE ASKING THE WRONG QUESTIONS! WE CAN HELP!

RESOURCES

- Brochures
- Infragard
- Videos
- WWW.FBI.GOV
- Call the Baltimore Field Office of the FBI
- SA Philip Todd: PHTODD@FBI.GOV

