RED DART ALLIANCE

U.S. Charges Three Researchers with Lying About Links to China

Source: BBC News, By Zhaoyin Feng, 28 January 2020

The US has charged a Harvard professor and two Chinese researchers based in Boston with assisting the Chinese government.

Harvard department chair Charles Lieber is accused of lying about his connections, while the researchers were charged with being foreign agents.

Mr Lieber allegedly accepted more than $1m in grant money from the Chinese government.

Harvard University called the charges against him "extremely serious".

In a statement, the university added: "Professor Lieber has been placed on indefinite administrative leave.

Who else was charged?

Prosecutors said Yanqing Ye, a Boston University robotics researcher, concealed the fact that she was in the Chinese army.

Ms Ye is accused of falsely identifying herself as a student and also continuing to work for the People's Liberation Army, while completing a number of assignments in the US.

Cancer researcher Zaosong Zheng was arrested at Boston Logan International Airport with 21 vials of biological samples in his bag. Prosecutors allege he was planning to return to China to continue his research there.

What were the alleged connections?

Court documents allege Mr Lieber, who has worked as the head investigator at the Lieber Research Group at Harvard University, received more than $15m (£11.5m) in grants from the US National Institute of Health and the US Department of Defence.

Recipients of these grants have to disclose any conflicts of interest, including financial support from foreign governments or organisations.

However in 2011, allegedly without Harvard's knowledge, Mr Lieber joined Wuhan University of Technology in China as a scientist.

According to the court papers, he also participated in the Thousand Talents Plan, a programme that aims to attract foreign research specialists. The US has flagged the programme as a security concern in the past.

From his role at Wuhan University of Technology, Mr Lieber was given a monthly salary of $50,000, in addition to living expenses of up to $158,000.

The filings say he was also given more than $1.5m to establish a research lab at Wuhan University of Technology and, in return, was expected

Continued on Page 2

U.S. Charges Three Researchers with Lying About Links to China

Continued from previous page

To work for the University, applying for patents and publishing article in its name.

'Hysteria' or 'non-traditional espionage'?

China says its Thousand Talents Plan is designed to keep "high-end talent" at home, in order to prevent a brain drain. The country has been losing talent to places like the US and the UK, where hundreds of thousands of Chinese attend top universities and subsequently settle down.

But the US view is that China is repeating a notorious tactic in its development playbook: intellectual property theft. For decades, Washington has accused Beijing of stealing science and technology from the US in order to gain an competitive advantage.

The FBI warns that the Thousand Talents Plan could be used by Beijing as a channel to conduct "non-traditional espionage", though many reported cases are not related to spying, but violations of ethics, such as not fully disclosing financial conflicts of interest.

Washington has increased its scrutiny on China's Thousand Talents Plan since 2018, when the two countries started to be locked in a trade battle, and Beijing has reportedly refrained from talking publicly about the program.

Chinese state tabloid Global Times labelled the American scepticism as "hysteria".

Since 2008, more than 7,000 researchers and scientists based outside of China have participated in the Thousand Talents Plan, many of whom are of Chinese descent.

Many warn that Washington's crackdown efforts must not give way to racial profiling. David Ho, a renowned Taiwanese-American HIV researcher, suggested in an earlier media interview: "If you want to implement policies, you should implement for all, not just the Chinese scientists."

Worth Checking Out

CNAS

The Center for a New American Security (CNAS) is an independent, bipartisan, nonprofit organization that develops strong, pragmatic, and principled national security and defense policies. CNAS engages policymakers, experts, and the public with innovative, fact-based research, ideas, and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

To see some of their reports go to

https://www.cnas.org/reports

The Homeland is Not a Sanctuary Admiral Warns Russia and China Can Target U.S. Navy in American Ports

Source: The Washington Examiner, By Joel Gehrke, 04 February 2020

Russia and China have the ability to attack U.S. Navy equipment when it's docked in American ports, a top admiral warned while discussing Washington's intensifying rivalries with Moscow and Beijing.

“The homeland is not a sanctuary,” Vice Adm. Andrew "Woody" Lewis said on Tuesday at the Center for Strategic and International Studies in Washington.

Lewis, who leads Joint Forces Command Norfolk and the Navy's newly reactivated 2nd Fleet, has been tasked with protecting the Atlantic from “great power” rivals such as Russia and China. The fleet, a mainstay of American defenses during the Cold War, was mothballed in 2011 and then re-established in 2018 as the United States's relationship with Russia deteriorated.

...it will be driven by investments in gray matter as much as gray hulls

“Our new reality is that when our sailors toss lines over and set sail, they can expect to be operating in a contested space once they leave Norfolk,” he said. “We are seeing an ever-increasing number of Russian submarines deploy in the Atlantic. And these submarines are more capable than ever, deploying for longer periods of time with more lethal weapons systems.”

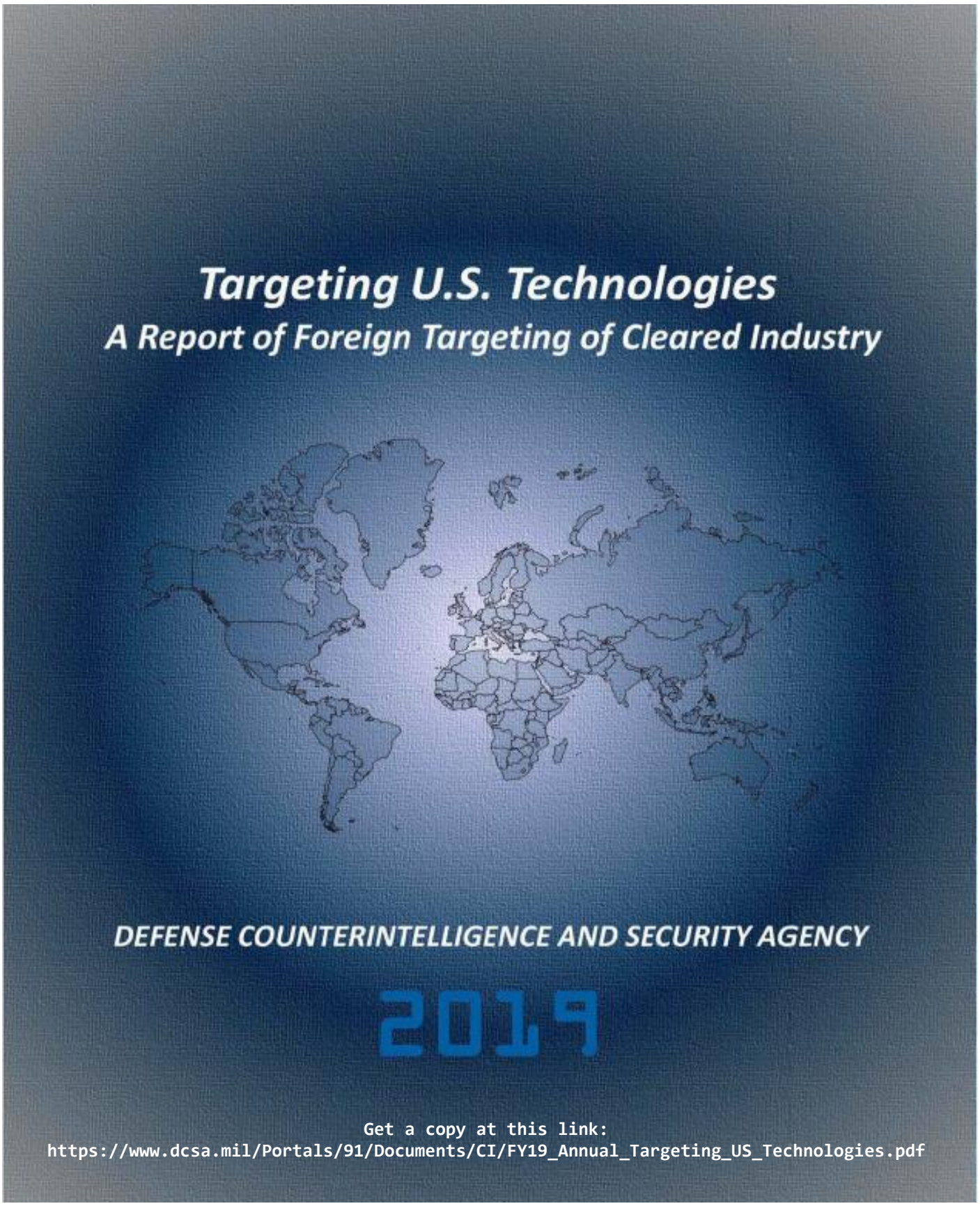
New technologies provide unexpected ways to threaten the Navy, such as “quadcopters” and other “small unmanned aerial systems” (that is, drones) that “can present a potential threat to forces” even before a ship is underway.

American strategists and tacticians need to get creative in planning how to stymie such threats because the Navy doesn’t have the kind of overwhelming military edge that U.S. forces enjoyed in recent decades, he said. “I believe that there's an awakening amongst our sailors that there are real bad things, potentially. ... Where we take a lot of risk nowadays is in our cybersloppiness, for lack of a better term.”

“If we were to look at how great power competition will be driven, it will be driven by investments in gray matter as much as gray hulls,” Lewis added. “The gap that we'll have on a technological basis, weapons systems, will not be that great. It's how we fight.”

The admiral’s comments amplified Pentagon warnings that Russia and China are developing plans to block U.S. forces from key ports around the globe and to threaten American troops long before they arrive on the scene of a crisis.

“Our ships can no longer expect to operate in a safe haven off the east coast or merely cross the Atlantic unhindered to operate in another location,” Lewis said.



Get a copy at this link:
https://www.dcsa.mil/Portals/91/Documents/CI/FY19_Annual_Targeting_US_Technologies.pdf

Israel's NSO: the Shadowy Firm Behind the 'Chilling' Spyware Used to Hack WhatsApp and Cloud Services

Source: The Telegraph, By Matthew Field, Hasan Chowdhury and Raf Sanchez, 30 October 2019

For campaigners and lawyers targeted by nation state cyber surveillance, the watchful eye of an authoritarian regime can feel impossible to escape.

"I first started noticing these weird calls in March," one human rights lawyer told The Telegraph. "It was video calls on WhatsApp, these calls were three or four seconds and by the time you get to the phone the call is gone."

Random calls are common enough and are usually benign, but when you're a lawyer representing Mexican and Saudi dissidents who have previously been targeted by spyware, a succession of mystery calls in the early hours of the morning from Sweden, Iceland and Ireland offered understandable cause for alarm.

The lawyer, who requested anonymity, is among a string of people who believe they have been targeted by Pegasus, a powerful smartphone virus developed by a shadowy Israeli security company and sold to security forces around the world.

In the murky world of digital espionage, Pegasus is not the winged horse of Greek mythology, but a devastating cyber weapon.

The software has allegedly been used to remotely target users over WhatsApp, and has recently been reported to have the capability to break into users cloud storage on services like Google Drive and iCloud .

Human rights groups claim the Israeli company behind the WhatsApp hack is linked to efforts to crack down on activists and journalists in the region CREDIT: ALAMY

Continued on Page 6

Israel's NSO: the Shadowy Firm Behind the 'Chilling' Spyware Used to Hack WhatsApp and Cloud Services

Continued from previous page

It is the flagship software of Israeli private security company NSO Group Technologies, a company that deals in "chilling" hacks to spy on smartphones.

The software is described by NSO co-founder Shalev Hulio in suitably mythic terms. Pegasus is the company's "Trojan horse" that could be sent "flying through the air to devices" and infiltrate them, he says.

Founded in 2010, the Herzliya headquartered company is currently valued at $1bn and employs 500 cyber security experts. Hulio, the company's chief executive, spent his time in the army in a search and rescue unit, before creating the company with Omri Lavie.

NSO's website says it develops spying technologies to help "government agencies prevent and investigate terrorism" saving "thousands of lives."

But according to human rights agencies, cyber security experts and Middle East activists spoken to by The Telegraph, the company's technology is linked to efforts to crack down on activists and journalists in the region.

It is accused of allowing its tool to be used to target activists and create a virus able to infiltrate WhatsApp, a messaging app used by 1.5 billion people. That spyware gives hackers full access to a target's phone, including their camera and microphone.

"The NSO are no amateurs at this and stop at nothing," says Jake Moore, a cybersecurity specialist at Slovakian security firm Eset.

According to Citizen Lab at the University of Toronto, NSO's Pegasus software has been detected in 45 countries. In six states at least, members of civil society had become targets, Citizen Lab says.

And increasingly, companies like NSO have been used as a diplomatic sales pitch to Israeli neighbours in the Middle East and the Gulf.

While Israel has no formal diplomatic relations with its Gulf Arab neighbours like Saudi Arabia, the two sides have drawn increasingly close in recent years and are cooperating on a range of security issues.

The relationship is driven partly by their shared opposition to Iran. But it is also fueled by the Arab states' interest in acquiring Israeli security technology like NSO's spyware, which they see as a powerful tool against terrorists but also political dissidents.

The company does not deny that it provides its services to Saudi Arabia, although it says strenuously that its technology was not used against Jamal Khashoggi, the Washington Post journalist murdered by Saudi operatives last year.

However, Saudi intelligence agencies armed with NSO spyware appear to have gone after several of Khashoggi's associates. Among them is believed to be Iyad el-Baghdadi,

Continued on Page 7

Israel's NSO: the Shadowy Firm Behind the 'Chilling' Spyware Used to Hack WhatsApp and Cloud Services

Continued from previous page

an Arab freedom activist. The CIA recently warned that Mr Baghdadi was being targeted by Saudi Arabia.

Mr el-Baghdadi said he was careful about his digital safety and never clicked links to try to keep his devices free from NSO spyware. "But then they upped their delivery mechanisms, including what we just found about Whatsapp, to the point that it's impossible to keep yourself safe," he told The Telegraph.

In May, NSO was accused in a court filing of "chilling attacks" on human rights activists by Amnesty International. The campaign group is calling for an export ban on NSO's technology to prevent it being used for breaches of the human rights act.

Amnesty pointed to one of its own researchers who it believed had been targeted by NSO technology. A source close to Amnesty said it believed the attack originated from Saudi intelligence forces. A separate attack was also detected against a UK lawyer working on a human rights abuse case in Mexico.

For its part, NSO's chief executive Hulio says the company has performed tests to ensure its products were not used in the murder of Khashoggi, which he called "a shocking murder", according to Israeli news site Ynet.

NSO says it strictly vets its clients and would not allow its tools to be used against activists. It said its technology is "solely operated by intelligence and law enforcement agencies". It has also said its tools are not used for "hacking or mass-collection" from cloud services.

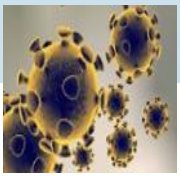
But el-Baghdadi and Amnesty lawyers have both called on Israel to support a tighter control on NSO technology, to prevent it being sold to oppressive regimes. But the prospect of change seems unlikely. For el-Baghdadi, it will be up to technology companies to use full legal force in dealing with these hacking arms deals.

"I think the tech companies themselves need to be extremely concerned about this. Someone has to tell this company to back off," he said.

While most ordinary people can happily keep using WhatsApp without fear of being spied on by a foreign state, for el-Baghdadi, that is a daily risk. "I am continuing under the assumption they could hack me at any moment," he says.

An NSO spokesman said: "We investigate any credible allegations of misuse and if necessary, we take action, including shutting down the system. Under no circumstances would NSO be involved in the operating or identifying of targets of its technology, which is solely operated by intelligence and law enforcement agencies. NSO would not or could not use its technology in its own right to target any person or organization, including this individual."

Tip of the Month



Some sites to find resources for Business Contingency Planning for Pandemics and Updated information about COVID-19:

The Center for Disease Control:

https://www.cdc.gov/flu/pandemic-resources/archived/business-planning.html

The National Institutes of Health:

https://www.nih.gov/health-information/coronavirus

The World Health Organization:

https://www.who.int/emergencies/diseases/novel-coronavirus-2019

U.S. Department of State China Travel Advisory:

https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories/china-travel-advisory.html

SCIENCE AND TECHNOLOGY

WHERE ARE WE?

Five emerging technologies will potentially transform society.

1. Genome Editing

Genome editing: A technique used to make specific and intentional additions, deletions, or alterations to genetic material. It could:

- prevent, treat, or cure medical conditions
- create unintended and unforeseen genetic changes in the population

2. Artificial Intelligence and Automation

Artificial intelligence (AI) could:

- produce smarter machines that perform more sophisticated tasks
- disrupt the job market by eliminating jobs and creating others with new skill requirements

While its use is expected to grow, AI that is as intelligent as a human is not expected to occur in the next 20 years.

3. Quantum Information Science

Quantum information science: uses the behavior of atoms or molecules to obtain and process information in ways that existing systems cannot. It could:

- drastically improve information acquisition, processing, and transmission

4. Brain/Augmented Reality

Brain-computer interfaces: systems that connect the human brain to an external device. Research is ongoing to create implantable versions that could, for example, compensate for vision loss or hearing impairment.

Augmented reality: superimposing a digital image onto a view of the real world through a device, such as a smartphone camera. It is a new trend in entertainment, education, and health care.

5. Cryptocurrencies and Blockchain

Cryptocurrencies: virtual currencies—digital representations of value that are not government-issued—that operate online and verify transactions using a public ledger called **blockchain**.

Cryptocurrencies offer:

- benefits such as anonymity and lower transaction costs
- drawbacks such as making it harder to detect money laundering and other financial crimes

Blockchain could:

- reshape financial services
- have more security vulnerabilities as quantum computing, an area of quantum information science, develops

WHAT ARE THE IMPLICATIONS?

Continued **debate, study, and evaluation** are needed in the public sector to consider the potential implications:

economic | ethical | privacy | safety | security | societal

For more information, see GAO-18-396SP at GAO.GOV.

GAO

Chinese 'Students' Keep Getting Arrested at Key West Navy Base

Source: Breaking Defense News, By Paul Mcleary, 29 January 2020

Dean Cheng, a China analyst at the Heritage Foundation, called the inept spywork "very strange," but noted similar acts are likely happening all across the United States.

Special Operators fast-roping aboard Canadian HMCS Moncton in Naval Air Station Key West's Truman Harbor.

WASHINGTON: Earlier this month, Yuhao Wang and Jielun Zhang, Chinese students at the University of Michigan, drove past a gate guard at Naval Air Station Key West after ignoring instructions to turn around, leading military police on a 30-minute chase that ended in their capture where investigators found pictures of military buildings on a camera and cell phone.

The incident came just weeks after another Chinese citizen, Lyuyou Liao, was charged with unlawfully taking pictures of military buildings on Key West after walking around a perimeter fence and getting inside the base from the water, ignoring warnings from people nearby that it was a restricted area. Liao claimed he was trying to take pictures of the sunrise, but investigators only found pictures of the Truman Annex on his camera.

We don't know exactly why the Chinese are paying so much attention to Naval Air Station Key West. While small, the base plays a big role in training, tech experimentation, and monitoring and tracking vessels offshore.

Navy F-18 pilots train there to sharpen combat tactics, and it is also used to train Navy detachments of Army, Navy, and Marine Corps special forces troops. Critically, it's also home to Joint Interagency Task Force South, which monitors illegal trafficking in the Caribbean by fusing Navy and Coast Guard air and sea operations while collecting intelligence in the region.

That mission — and the way it's organized and carried out — might be of interest to Beijing as it aggressively pushes past the first island chain and find itself having to contend with keeping watch over vast swaths of ocean. To keep its people connected, Beijing will need to mesh disparate operations and platforms together with multiple ships, aircraft and sensors in play. The task force is housed in the Truman Annex, which drew so much attention from Liao in December.

Key West was also recently used for testing new unmanned air and undersea systems the Navy is experimenting with, that may have caught Beijing's eye.

Continued on Page 11

Chinese 'Students' Keep Getting Arrested at Key West Navy Base

Continued from previous page

The interest by the Chinese government in how the US trains and equips its forces is hardly a surprise. The Pentagon has been warning for years that Beijing hacks into government and military contractors' networks to pull classified plans and sensitive acquisition data out for their own use. But what has caught many by surprise is the simplistic nature of the gate rushes, a far cry from the more tech-centric spying the Pentagon is scrambling to protect itself from.

China remains determined to steal American technology "at any cost," Defense Secretary Mark Esper said last week, warning that American companies remain under "continuous siege" digitally. Acting Navy Secretary Thomas Modly recently told me that "the Chinese have stolen a lot of [technology] from us, and they're pretty good at stealing from us and putting that right into platforms and things that can ultimately threaten us."

Dean Cheng, a China analyst at the Heritage Foundation, called the inept spywork "very strange," but noted similar acts are likely happening all across the United States. Cheng said the Chinese might be interested in seeing how the special operations forces on base train and equip since Beijing "is worried about what Special Operations are doing. They might look at that and think those guys might have a support Taiwan mission" in the event of hostilities.

A scene similar to those at Key West played out last fall when two Chinese diplomats and their spouses ignored the instructions of a gate guard at Fort Story, Va., leading to another chase that only ended when fire trucks were parked in their path. The New York Times reported that one of the diplomats was suspected of having ties to Chinese intelligence. Both were expelled in December.

The December and January incidents came about a year after the original Chinese gate runner, Zhao Qianli, got inside the complex in September 2018. He would eventually plead guilty to illegally taking photographs of Joint Interagency Task Force South, along with the command's secure Antenna Farm. Federal authorities would later claim he lied on his visa application, omitting this Chinese military service. Searching his Miami hotel room, investigators found a police uniform and the People's Republic of China Interior Ministry belt buckle which he claimed they were given to him by his father. He was sentenced to a year in prison, and released in November.

A spokesperson for Naval Air Station Key West would not talk about security measures at the base or any recent changes there but confirmed, "our mission here is to support warfighter training. We host aircraft and other squadrons/units from all services and agencies at our airfield on Boca Chica Field and in our Truman Harbor at Truman Annex. We mostly host a lot of F/A-18 Super Hornet squadrons for air-to-air combat training in our ranges to the south of Key West and in the Gulf of Mexico."

Continued on Page 12

Chinese 'Students' Keep Getting Arrested at Key West Navy Base

Continued from previous page

Another area of interest might be the existence of Fighter Squadron Composite 111 at Key West, an "aggressor" squadron that Navy and Marine Corps pilots train against. The squadron plays the role of enemy aircraft, giving fighter pilots a chance to practice air combat tactics, something China would love to see up close as its pilots push further out to sea on aircraft carriers and airstrips on man-made islands in the South China Sea.

From the Office for Victims of Crime: www.ovc.gov

2020 National Crime Victims' Rights Week (NCVRW)

The 2020 NCVRW Resource Guide theme artwork, theme poster, web artwork, and sample proclamation are now online. Use this content to help your organization promote NCVRW and awareness about victims' rights and services.

Visit our NCVRW website to view these materials.

National Elder Fraud Hotline

To help combat fraud against older Americans and provide services to victims, OVC announces the launch of the National Elder Fraud Hotline. Call 833–FRAUD–11 (833–372–8311) to receive help from a hotline case manager.

Learn more on the National Elder Fraud Hotline website.

Serving Victims in Tribal Communities

Visit the OVC Tribal Multimedia Resources page which offers videos designed to inform and assist victim service providers and allied professionals in their efforts to help crime victims in Indian Country.

Access resources.

Longer but Worthwhile Reads:

- **Chinese tech in U.S. funnels data to Beijing's intelligence services**

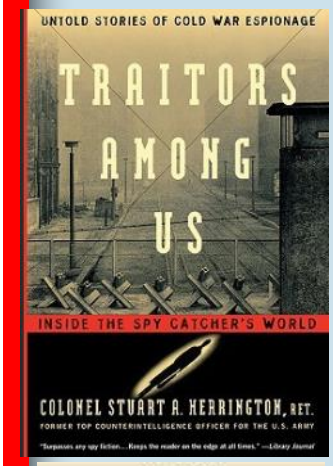
https://www.washingtontimes.com/news/2020/feb/24/lexmark-lenovo-tech-funnels-data-china-intelligenc/

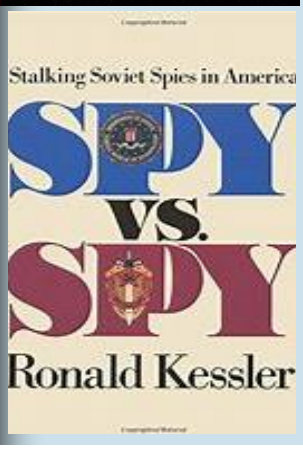
- **Harvard, Yale under investigation for $375 million secret funding from China, Saudi Arabia**

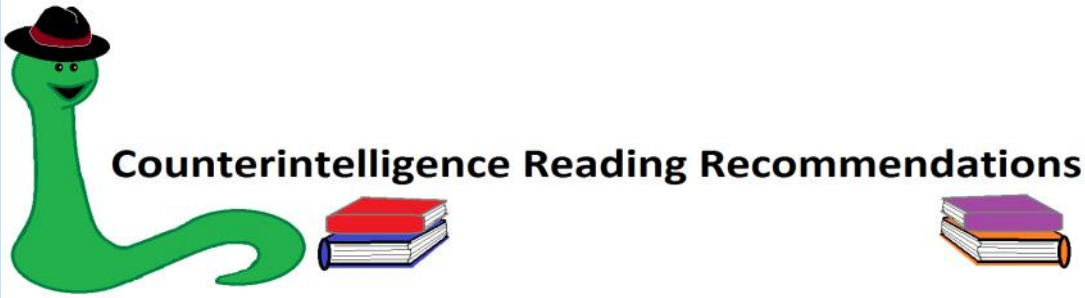
https://americanmilitarynews.com/2020/02/harvard-yale-under-investigation-for-375-million-secret-funding-from-china-saudi-arabia/

- **U.S. Charges 4 Members of Chinese Military with Equifax Hack**

https://finance.yahoo.com/news/u-charges-4-members-chinese-032914090.html







Traitors Among Us: Inside the Spy Catcher's World By Stuart Herrington

The story of Army Counterintelligence investigations of traitors Clyde Lee Conrad and James W. Hall III by Colonel Stuart Herrington (USA Ret), former Commander of the U.S. Army Foreign Counterintelligence Activity.

Spy vs. Spy: Stalking Soviet Spies in America *By Ronald Kessler*

Acclaimed journalist Ronald Kessler takes readers inside the deadly world of espionage and counter-espionage to reveal how Russian agents operate in the United States, how greedy Americans can betray top military secrets with astonishing ease, and why most Russian spies walk away free.

RED DART Agency Spotlight

U.S. Air Force Office of Special Investigations

Who we Are: An Air Force Field Operating Agency accountable to the Secretary of the Air Force under the guidance and direction of the Inspector General.

Mission: To Identify, exploit and neutralize criminal, terrorist and intelligence threats to the Air Force, Department of Defense and U.S. Government.

AFOSI is headquartered at Quantico, Va., but has units in 221 locations globally -- both on Air Force bases and in strategically important locations around the globe.

U.S. AIR FORCE

What we Do:

Why We Exist	Vision	Capabilities	Lines of Operation	Effects
Defend The Nation	A trusted and valued global investigative agency in sync with a changing strategic environment. A reliable partner, recognized for excellence, creating and protecting the USAF of the 21st Century *A Full Spectrum, Adaptive and Resilient Force*	Protect Secrets	Criminal Investigations	A Protected Force
Serve Justice		Detect Threats	Fraud Investigations	Neutralized Criminal Activity
Protect USAF		Specialized Services	Counterintelligence	Developed Partnerships
Find Truth		Conduct Investigations	Cyber	Acquisition Integrity
		Engage Foreign Threats	Expeditionary Activities	Enabled Force Engagement
			Special Security Services	Secured Technologies & Information
				Global Situational Awareness

We are a federal law enforcement and investigative agency operating throughout the full spectrum of warfare!

Eyes of the Eagle

U.S. AIR FORCE
EagleEyes
WATCH. REPORT. PROTECT.





Current RED DART Teams

* RED DART North Carolina * RED DART Southern Virginia * RED DART Huntsville * RED DART South Carolina

* RED DART Central Virginia * RED DART Gulf Coast * RED DART Chicago * RED DART North Texas

* RED DART North Mississippi * RED DART Indiana * RED DART Silicon Valley * RED DART South Florida

* RED DART Tennessee * RED DART Sacramento * RED DART Greater Los Angeles * RED DART Colorado

* RED DART Southwest Ohio * RED DART Hawaii * RED DART San Diego *RED DART Japan

The stated purpose of the RED DART program is to create a unified, cross-agency team of counterintelligence professionals dedicated to the protection of classified and sensitive technology research throughout a given area of responsibility (AOR). RED DART operates under a "shared leadership" principle, which allows each partner agency to own the program while being responsible and responsive to the other partner agencies.

Contact your servicing RED DART representative for additional information on the articles and information contained in this newsletter.

New RED DART teams are forming regularly throughout the U.S. Contact your servicing Defense Counterintelligence and Security Agency (DCSA) CI agent or Federal Bureau of Investigation (FBI) CI agent to see if a team is being established in your area.