Michael C. Casey
Director of the National Counterintelligence and Security Center (NCSC)
Office of the Director of National Intelligence (ODNI)

Remarks As Prepared For Delivery To:
The Economic Development Association of Alabama (EDAA)
Winter Conference
January 30, 2024
Montgomery, Alabama

INTRODUCTION

Thanks for that kind introduction Robert, and thanks for connecting us to this conference. I'd also like to thank Jim Searcy and the Economic Development Association of Alabama for inviting me to speak today.

As a proud University of Kentucky graduate, I can say it's great to be here in Alabama, particularly during basketball season. It's usually less welcoming for Wildcats in football season.

Now, let me start with a rhetorical question. Why is a counterintelligence official here speaking at an economic development conference? The answer: I'm here to help highlight risks.

I'd bet that not one of you would undertake a development opportunity without thinking through economic risks to the project. I'm just here to highlight some of the counterintelligence risks you might also want to consider.

The bottom line is -- you have to successfully navigate risks to realize opportunities.

My center wants you take advantage of the many opportunities in the global marketplace. We also want to help you navigate the risks. As you interact with foreign entities to bring investment to your state, we want you do it *securely and with your eyes wide open*.

Navigating the global business landscape has become especially challenging in recent years. Foreign adversaries are targeting virtually every industry in the U.S. to acquire data, technology, and talent to advance their own economic and national security goals. No U.S. industry or company -- small or large -- is immune.

And theft is not the only problem. Alabama and other states also face foreign influence. Across the U.S., we see entities backed by foreign governments trying to curry favor with U.S. business & government leaders at the state and local level.

They may promise jobs, lucrative investments or access to their markets, which is great. But sometimes foreign governments exploit these relationships to advance their own agendas -- at your expense and at the expense of the U.S.

The bottom line is we no longer live in a spy-versus-spy world. The days of foreign spies only targeting the U.S. government are over. Businesses, universities, local governments, and other organizations are now in the crosshairs of those seeking to gain advantage over the U.S.

In the theme of stealing foreign Intellectual Property, I'm going to borrow a line from one of my British counterparts – "You may not be interested in geopolitics, but geopolitics is interested in you," -- no matter your line of business.

That applies in Alabama and all across America.

Now that I've spoiled the mood, let me outline what I plan to talk about for the rest of my time.

- I'll start with a brief introduction of the National Counterintelligence and Security Center (NCSC), the organization I lead.
- Next I'll provide an overview of the global counterintelligence trends we see and the major threat actors involved.
- Then I'd like to focus on Alabama as a target of our adversaries. I'll touch on some of the key sectors they're targeting and the techniques they're using.
- I'd also like to talk about foreign influence schemes and how to guard against them.
- Finally, I'd like to close with some basic mitigation steps you can take to protect yourself.
- If we have time at the end, I'll be happy to try to answer questions you may have

NCSC OVERVIEW

For those of you unfamiliar with NCSC, we're a component of the Office of the Director of National Intelligence. Our mission is to lead and support the U.S. Government's counterintelligence and security activities.

Within the U.S. Government, our key functions include building insider threat programs, reforming the security clearance process, enhancing supply chain risk mitigation, and overseeing security standards and compliance for overseas diplomatic facilities.

We also produce the National Counterintelligence Strategy of the United States.

In addition, we have an important private sector outreach function, which is why I'm here today.

We try to help industry understand foreign intelligence threats to their organizations, provide information on risk mitigation, and empower them to take steps to enhance their own security.

GLOBAL CI THREAT TRENDS

Let me talk now about some of the global threat trends we see. The counterintelligence threat landscape can be summed up as … more, more, and more. Basically, counterintelligence is a growth business.

More adversaries: We face an expanding array of adversaries -- and not just the People's Republic of China (PRC), Russia, Iran, and North Korea – but also non-state actors such as ransomware groups, terrorist organizations, and ideologically motivated groups.

More tools: In addition, Russia, China, and other threat actors have increasingly sophisticated intelligence capabilities, technologies, and tools -- and they're using them in new ways to target the U.S. Much of this new technology is commercially available.

- You may have heard of the NSO Group that sells spyware around the world. They're not alone—commercial spyware is a big business and it helps unsophisticated intelligence services to become serious threats.

More targets: We also see threat actors going after more targets. Twenty years ago, our adversaries were mostly going after U.S. Government secrets. Today they've expanded their target list to include virtually every sector of our economy to acquire technology and talent to advance their interests.

More data: Data is one example of this expanded target list. Adversaries are increasingly targeting all kinds of data -- from personally identifying information, such as your social security number, to health and genomic data.

They view data as a strategic resource and collection priority, not only for their own economic advancement, but also for their intelligence and military operations.

China (which we call the PRC) is the most aggressive. The PRC has stolen more Americans' personal and business data than every other nation combined.

Like many Americans, I count myself as one of their victims. Three times they've snatched my personal data.

Now with all this data in the PRC's hands, one of our concerns is that they'll use artificial intelligence to aggregate it and help turbocharge their hacking and espionage activities.

More attack vectors: Moving on, we're also having to defend against more attack vectors from adversaries.

It's not just illicit tactics like cyberattacks and insider threats we have to worry about, but also legal and quasi-legal tactics, like mergers, acquisitions, investments, and joint ventures.

They're using legitimate business tactics to achieve illicit goals. We're also seeing blended operations that combine some or all of these elements.

More collaboration: Finally, we're also seeing adversary intelligence services increasing their collaboration with hacking groups and with one another, expanding their reach, and magnifying the threat.

KEY THREAT ACTORS

Let me talk now about the key threat actors. In terms of nation-states, China and Russia continue to dominate the landscape.

I want to be clear I'm talking about the Governments of China and Russia, not their general populations, who are often victimized by these regimes. I'm also not talking about Chinese-Americans or Russian-Americans.

The PRC today represents the broadest, most active, and persistent cyber espionage threat. They also remain the top threat to U.S. technology competitiveness.

- China is not just going after classified data, but unclassified data, technology and talent. They use every tool in the toolkit -- they may recruit an insider, use a cyber intrusion, make an investment, recruit top talent, or do some combination of all of those things, to get what they want.

And, despite their military losses in Ukraine, no one should underestimate the Russian intelligence services. They remain a formidable threat to the U.S. and its allies.

- Russia continues to target the U.S. through espionage, influence operations, and cyber activities, while also seeking to degrade U.S. and partner support for Ukraine.

As you know, Iran, North Korea, and a variety of other nation-state actors also pose major threats, but in the interest of time, I'll skip over them.

ALABAMA AS A TARGET

So what does all this mean for Alabama? The good news is Alabama is home to a thriving, business community. The bad news is this community is an attractive target for adversaries.

Alabama is a leader in aerospace, with more than 300 aerospace companies from more than 30 countries and tens of thousands of aerospace jobs. Alabama is also nationally recognized for its aerospace education, talent, and research facilities.

Alabama also has a booming automotive sector and is poised to become a leader in the production of graphite, a key component for lithium batteries and Electric Vehicles. Graphite is critical to America's energy future.

Alabama's bioscience sector also hosts some of the nation's top research facilities, employs some 18,000 people, and generates more than $7 billion in economic impact.

On top of all that, you have vital agriculture, chemical, and other industries in Alabama -- not to mention all the U.S. military bases here and the industries that support them.

All these are collection priorities for adversaries. Russia and other nations target these sectors. But nobody goes after them like the PRC.

Through national industrial plans like Made in China 2025 and the 14th Five Year Plan, the government of China has made clear it seeks to achieve global dominance in a broad range of industries in the near future.

China's national plans have become roadmaps for PRC theft across the U.S. Whether it's cancer research or precision agriculture, if it can help them gain an advantage, they'll go after it.

The Chinese government has literally told us what they're after. We should probably take them at their word.

AEROSPACE SECTOR AS AN EXAMPLE

As an example, let me talk to those in the aerospace sector.

Several recent developments prompted us, the FBI, and Air Force to issue a renewed warning last August about foreign intelligence threats to this sector.

First, the tremendous growth in the commercial space industry makes it ripe for economic espionage.

The global space economy is expected to grow from $469 billion in 2021 to more than $1 trillion by 2030, with the U.S. as the main driver of this growth. This is significant for Alabama, which in 2022 alone was the recipient of some $1.2 billion in new aerospace investment.

The PRC understands this. China routinely targets commercial U.S. space companies to acquire technology and talent to fill gaps in their own space program, as they attempt to gain supremacy in space.

And they're also testing weapons that could potentially disable or hijack satellites that the U.S. military and U.S. businesses rely on to operate around the world.

The conflict in Ukraine, which highlighted the target on the backs of some U.S. space companies, also helped prompt our warning. Our adversaries view any number of U.S. space companies as potential threats to them.

In 2022, at the onset of the war in Ukraine, Russia carried out a major cyberattack on ViaSat, an American satellite communications company based in California.

The Russians weren't trying to steal ViaSat's technology or data. They were trying to knock out ViaSat's satellite communications services because Ukraine used them for command and control of its troops.

This was a watershed moment for the commercial space industry and for the U.S. Government as well….a concrete example of a foreign government attacking a U.S.-based satellite company that played out in real time, in a real conflict.

Russia's attack on ViaSat had major downstream effects, impacting more than 5,000 wind turbines in Germany and disrupting internet access for thousands of others across Europe.

A final reason we issued our warning is that adversaries understand just how reliant the U.S. has become on commercial space companies.

They know U.S. space assets play a key role in sectors like emergency services, financial services, telecoms, transportation, and agriculture. In a conflict, the targeting of U.S. assets in space would have huge impacts.

Example -- GPS satellites are owned by the U.S. government, but just imagine the chaos if they were taken out. Yeah, the Google Maps on my cell phone wouldn't work, and some of us might not be able to find our way to the grocery store. But we would all face much bigger problems.

All manner of planes, trains, ships, cars, and trucks rely on GPS for location data. And our cellular communications and financial transactions also rely on GPS timing signals. All would be impacted.

The bottom line is adversaries today see U.S. space innovation and assets as potential threats to them, as well as valuable opportunities to acquire vital technologies and expertise.

For these reasons, we're working closely with FBI, Air Force, and other agencies to raise threat awareness in this industry and provide risk mitigation information.

ADVERSARY TARGETING TECHNIQUES

OK, let me pivot now and highlight some of the different ways threat actors target U.S. industries, including those in Alabama.

As I explained before, their tactics range from the illegal -- like cyber intrusions and recruiting insiders at companies to steal data….to quasi-legal and even legal tactics -- whereby they acquire data through seemingly legitimate investments, partnerships, joint ventures, or regulatory actions.

I've already mentioned cyberattacks in the context of commercial space, so let me touch on insider threats as an attack vector.

Insider threats are employees of an organization who use their authorized access to harm that organization, either wittingly or unwittingly.

Every organization is vulnerable to insider threats. The U.S. government has had its fair share of insider threats – just remember Edward Snowden.

Today, our adversaries continuously target and recruit insiders at U.S. companies to acquire data and technology.

Their targets can be almost anyone with access to data they want, and a vulnerability they can exploit. It may be an employee who has financial problems, or is angry at their boss, or is just naïve on social media and has bad cyber hygiene.

Nation states are particularly adept at recruiting insiders on social media, professional networking sites, and other job platforms. Russia and North Korea use these techniques, but, again, the PRC may be the most prolific.

In October, Britain announced that PRC operatives had targeted more than 20,000 Britons via fake profiles on LinkedIn for recruitment or information gathering.

Threat actors often pose online as headhunting companies and use flattery to establish a relationship with targets. They may offer paid consultancy work or ask people to write 'white papers,' then follow up with requests for non-public data.

They may also post job ads online and let targets apply. For promising targets, they may offer paid trips abroad for meetings. Once abroad, the target can be compromised and pressured to turn over more.

To help guard against these threats, we encourage all organizations to have an insider risk program. Good insider risk programs train their employees on these types of threats. In the government, we call them Insider Threat or Insider Risk programs, but really a lot of what they do are employee wellness.

These programs encourage employees to speak up when they see concerning behaviors at work. This can help organizations intervene early before a negative event occurs. It can also result in positive outcomes for at-risk employees, getting them help before they go down a dark path.

Moving on from insider threats, let me highlight some of the legal and quasi-legal techniques used by our adversaries.

Malign investment schemes are one area of concern for us.

We see foreign governments and companies beholden to them using a variety of investment schemes to gain access to emerging technologies they want for their own economic and military development.

This can include leveraging venture capital (VC) investments, investments through entities based in third countries, investments as limited partners, and iterative minority investments.

For instance, we see VC investment in U.S. startups by entities in third countries that go to great lengths to hide their ties to hostile governments. Even a minority investment in a tech start up can give a threat actor some influence or access.

It's critical for U.S. tech companies to conduct due diligence on potential investors to determine their funding sources and motivations. When in doubt, or if you have concerns, please reach out to your local FBI office.

And on the legal & regulatory front, if you're doing business in China, be aware that in recent years, the PRC has enacted comprehensive national security, cybersecurity and data privacy laws that greatly expand its oversight of foreign companies operating there.

These laws give the PRC government expanded legal grounds for accessing and controlling data held by US firms in China.

A few years ago, the Chinese authorities required several US companies in China to install software to make tax payments. Surprise, surprise, the companies found malware embedded in that software, which created backdoors on the U.S. company networks.

The PRC has also passed laws that require Chinese companies to cooperate with the PRC intelligence services without the need for a warrant or any other legal process or notice.

If you're partnering with one of these companies, understand where your data could end up.

And finally, let me talk about joint ventures. U.S. companies often have to form joint ventures with Chinese state-owned entities as a condition of doing business in China. Unfortunately, many of these partnerships have been exploited in the past.

In the mid-2000s, for example, a Chinese state-owned entity called China Rail Rolling Stock Corp (CRRC) entered into joint ventures with several Western companies and benefited from their expertise and technology in the rail industry.

CRRC received major subsidies from the Chinese government, allowing it to undercut its competitors as it expanded.

Within a decade of entering Australia, CRRC wiped out Australia's domestic rail manufacturing entirely. Today, CRRC controls more than 80 percent of the global rail market.

FOREIGN INFLUENCE

Before I close, I want to talk about foreign influence. Russia, China, Cuba, Iran, and other nations all engage in influence operations in the U.S.

Many of us think about foreign influence in the context of foreign land purchases, elections, or wedge issues -- but it goes beyond that.

Some of the foreign influence that we see at the U.S. state and local level can be much more subtle and hard to detect, but just as problematic.

Unfortunately, the PRC Government has been among the most aggressive in attempting to exert influence in U.S. state and local communities -- and that's partly because of China's already deep economic ties to our cities and states.

For decades, entities across China have forged ties with U.S. state and local communities. These ties have often yielded economic and cultural benefits for both sides, which is a good thing.

But as tensions between Beijing and Washington have risen, the PRC government has increasingly sought to exploit these relationships to influence U.S. policy and advance their own interests.

Beijing may believe U.S. state and local leaders are more susceptible to PRC influence than Washington -- given these leaders' relative independence and focus on local economic issues.

And they may try to use these leaders as proxies to advocate for national U.S. policies that Beijing desires.

Some of this activity is overt, where the role of the PRC government is open. We've seen PRC consular officials asking local officials to introduce or pass measures aligned with Beijing's economic interests.

…or PRC diplomats making requests of business leaders. In 2021, the PRC Embassy asked numerous U.S. business executives with financial interests in China to actively lobby Congress against U.S. bills the PRC opposed.

Other influence operations can be deceptive -- with seemingly benign business opportunities or people-to-people exchanges masking PRC government agendas.

Financial incentives such as free trips, lucrative investments, or access to China's market may be used to hook local U.S. communities. And these incentives can create economic dependencies that the PRC can use as leverage to coerce behavior.

So what do these efforts at coercion look like?

Example -- A top official in one U.S. state was planning a trip to Taiwan – a democracy China is quite unhappy with. He was soon contacted by a PRC official who threatened to cancel a Chinese investment project in his state if he went to Taiwan. To his credit, the official resisted the pressure and went anyway.

This effort failed, but it shows you some the economic levers they may use for influence. Some other tactics we're worried about include:

- The PRC collecting personal data on state & local leaders (and those close to them) to find suitable influence targets;

- Recruiting officials early in their careers to exploit when they reach higher office;
- Exploiting friendship partnerships, like sister city programs, with U.S. communities;
- Creating economic dependencies in communities that they can use for leverage, and
- Targeting local business leaders as a vector to pressure policy makers.

It's important not to cast blanket suspicion on all outreach from China. Some of what I have highlighted are tactics that multiple countries use or is for legitimate business purposes—everyone lobbies about tax laws.

But these engagements can be exploited to undermine the U.S. or our economic advantages, and you should be aware of the risks.

Again, this threat comes from the PRC government and the Chinese Communist Party. It's not about the people of China generally or Chinese Americans, who themselves are often targeted by PRC aggression.

Look, we know it's essential for many U.S. communities to trade and engage with China. China is the second largest recipient of Alabama's exports.

We want Alabama to benefit from these opportunities, but also understand that, based on their record, the PRC government may seek to exploit some of these relationships for their own ends.

DISINFORMATION EXAMPLE

As a footnote to this discussion on influence, I would add that some foreign influence operations are designed to punish competitors -- rather than influence policy.

Let me give you one example --- which could potentially be relevant for the graphite mining and processing operations under development in Alabama.

China has a near-monopoly on rare earth elements and other minerals that are key components for Electric Vehicle batteries and other technologies. This gives them significant leverage in global markets.

To protect their dominance, we've seen the PRC trying to undermine competing rare earth companies around the globe with disinformation campaigns.

Recently, researchers exposed a China-linked social media campaign to spread disinformation about U.S., Australian, and Canadian rare earth companies to damage their reputations. The cyber actors targeted people in communities where these firms were building rare earth mines.

In Texas, for instance, the disinformation campaign used fake social media accounts, pretending to be Texans, to claim a rare earth project in the state would expose residents to radiation and environmental damage. The goal was to incite local opposition to the plant in Texas.

In Malaysia, they targeted an Australian mining company by posting to social media doctored photos of people suffering an array of medical conditions -- which they falsely attributed to the Australian mining company. Again, the goal was to stir up local opposition to the project.

Fortunately, these social media campaigns didn't get a lot of traction. But they show the growing sophistication of Chinese disinformation efforts and how they'll go after private companies competing with them in the global marketplace.

This can have a major impact on a company's bottom line and is something to pay attention to going forward.

BASIC MITIGATION TIPS

So I'll wrap up with what I believe is some good news. There are some basic steps you can take to mitigate risks. They're not silver bullets, but they will go a long way in hardening defenses.

I'll start with some basic tips for businesses.

As a first step, get to know the Private Sector representative at your local FBI field offices. Don't wait for a crisis to hit; establish a relationship now. Work with them to keep up to date on current threat information and security best practices. This can help you get ahead of threats.

Next, and perhaps most important: identify, prioritize, and commit to protecting your "crown jewels," the thing that makes your business successful.

When entering into deal with a foreign entity, think about the risk that your data, technology, or talent may be siphoned out. I've talked a lot about the PRC, but they're not the only country that steals Intellectual Property.

We also recommend businesses institute a comprehensive, enterprise-wide security posture. That means not leaving all the threats up to your security people. Include your acquisition, procurement, legal, and human resources offices in security planning. It's important for all these offices to collaborate to be effective.

And, as I noted earlier, we would recommend all organizations have an insider risk program to help them deter, detect, and mitigate potential threats coming from within the workforce.

It's also important to know who you're doing business with. This means scrutinizing your suppliers and setting minimum security standards for them. It also helps to diversify your supply chains to reduce dependencies. A single supplier is a single point of failure.

And before partnering with any foreign entity, check into their motives, funding sources, and whether they're subject to foreign government control or authority. Ensure transparency, reciprocity, and accountability are baked into the agreement.

Also be mindful of hidden strings that could be attached to a foreign partnership …

- Like requests for you to advance a position or lobby on behalf of the foreign partner …

- Or requests for you to stop interacting with people, entities, or countries that the foreign partner doesn't like. Recall the Taiwan example.

Finally, think about whether the partnership or project could create a financial dependency in your community that foreign entities, including foreign governments, could use as leverage to advance their agendas.

Cyber security and hygiene are also critical for your organization. All of us must patch regularly, use multi-factor authentication, monitor our systems, and protect our credentials.

It's also a good idea to maintain an "enigma list" of unexplained events or anomalies and periodically review to detect patterns. And tabletop exercises to plan ahead for worst-case scenarios can be extremely useful.

Given that your individual employees or executives can be targets these days, we also provide some basic counterintelligence tips to individuals.

When on social media, do your best not to accept online invitations to connect from people you don't know. Understand that what you post on social media about your work and contacts could draw unwanted attention from threat actors.

In terms of personal cyber hygiene, always be mindful of spear-phishing, which has become very sophisticated these days. Don't click on that suspicious link or attachment. Again, use multi-factor authentication and strong passwords.

Finally, if you're traveling abroad, you really can't expect privacy on your electronic device. It may be hard, but get a temporary phone for the trip. Leave that work or personal device at home, as those devices contain all your data.

And when you're on that trip, not a good idea to leave electronic devices unattended. Those hotel safes are never "safe."

I know that's an awful lot of information to process in this short period of time. But you're not alone in this effort.

If you have questions or concerns about a foreign entity, please reach out to your local FBI offices. In addition, many other U.S. cities and states face similar challenges when it comes to foreign engagements. They too can be a resource.

CLOSING

With that, I thank you once again for inviting me to speak with you today.

I hope I haven't dampened everyone's mood, but it's vital that you understand these threats so you can better prepare to navigate them.

And as the Director of NCSC, I want NCSC to be a resource and partner for you.

Please reach out if you have any questions – we have an abundance of threat mitigation resources available on our website at NCSC.GOV

And if we can't assist, we have parters at FBI and across the government who we can introduce you to.

I'm happy to try to answer any questions you have.