NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Advancing Counterintelligence and Security Excellence

Remarks as Prepared for Delivery

Mirriam-Grace MacIntyre
Executive Director, National Counterintelligence and Security Center
at the
Intelligence Community Centers for Academic Excellence (IC CAE)
Principal Investigators Development Summit
San Antonio, Texas
February 21, 2024

INTRODUCTION

Good afternoon. It's an honor to be here with you today and to share a bit about the work my organization does. The work you do at your institutions is so critical to the strength of our nation and to growing the next generation of national security leaders. So, I want to thank you for that.

As we seek to "Connect, Advance, and Engage," I hope to give you a flavor of our work, a sense of how we might expand students' understanding of counterintelligence, and identify ways we can further partner.

Let me start by talking about counterintelligence, which is the bread and butter of the organization I represent, the National Counterintelligence and Security Center (NCSC).

Counterintelligence—or CI— can basically be summed up as activities designed to prevent or thwart espionage, intelligence gathering, and sabotage by an adversary or other foreign entity.

To many, this conjures up images of gun-toting agents tracking spies in the shadows. For others, perhaps those of you who spent time in our community, your thoughts may be limited to internal security functions divorced from mission.

The reality is that while gritty, spy-versus-spy work certainly still goes on, counterintelligence has evolved dramatically and become more multi-dimensional over the past 20 years.

Today, our adversaries are no longer just interested in classified information or government secrets. They seek almost any type of research, data, technology, or innovation that can advance their economic or national security goals at our expense.

That means unclassified information -- ranging from scientific research at universities, to personal data on your laptop, to intellectual property at companies -- is at risk. Over the past decade, almost every sector of our economy has become a target. No university or company – large or small is immune.

Protecting this broad range of targets makes our jobs in the CI community far more challenging and it means that **partnerships** and **people** are more essential to accomplishing this work.

The partnerships we have with academia and industry form the backbone of our collective defense. We do our best to help these organizations understand the threats they face and give them the tools and information they need to harden their defenses.

On the people front, we must also have a healthy pipeline of young talent from diverse backgrounds to help us build our workforces to meet the CI challenges of today and tomorrow.

In short, everyone, including your students and academic institutions, has some role to play in protecting our nation from today's emerging CI threats.

NCSC OVERVIEW

As we seek to connect, let me talk briefly now about the organization I have the privilege of leading and how we fit into this ecosystem.

NCSC is a component of the Office of the Director of National Intelligence. We're charged with leading and supporting the U.S. Government's CI and security activities.

Practically speaking, this means that we help agencies build insider threat programs, reform the security clearance process, mitigate supply chain risks, oversee security standards and ensure overseas diplomatic facilities meet the highest security standards to match the threat.

We also develop and issue the National Counterintelligence Strategy of the United States, which is signed by the President. Our team brings the best of the best from across the IC to lead coordinated efforts to achieve the strategy's goals.

In addition, we have an important outreach function. We develop threat awareness products for the private sector, as well as academic and research organizations, to help them understand foreign intelligence threats to their organizations. We provide them information on risk mitigation and try to empower them to enhance their own security.

NCSC AS A PLACE TO WORK

With such a wide-ranging mission, attracting the right talent is critical.

Our team is mission-focused, collaborative, and the opportunities abound. In fact, I'm proud of the fact that our center often ranks at the top of job satisfaction scores on ODNI's climate survey.

At the same time, our broad CI and security mission areas involve some of the most diverse and interesting fields you can imagine. That's because countering foreign threats involves everything from strengthening IT supply chains to safeguarding science.

- We have human behavioral scientists who work to improve personal vetting and insider risk practices for the government.
- We have scientists and technical experts working to counter some of the most advanced technical collection techniques of our adversaries.
- We also have experts in emerging technologies, such as biotech, AI, and semiconductors, given our adversaries' growing focus on these areas.
- One recent FBI detailee to NCSC had a prior career in molecular biology and human gene therapy. For us, he was a critical ambassador to the biotechnology community in helping them mitigate threats to their sector.
- And we even have our fair share of political science, sociology, and international affairs majors.

As Executive Director, I'm responsible for overseeing the Center's day-to-day operations and, from my perch, I get to see all these people from diverse, interesting backgrounds come together for a common purpose and enhance one another's perspectives with the diversity each one brings.

To support our CI mission in the coming years, we need a workforce with a broad array of skills—from liberal arts majors to specialists in science and engineering, particularly in STEM subject areas.

As we all know, STEM occupations are projected to grow over two times faster than all other occupations in the next decade. STEM opportunities at NCSC and across the Intelligence Community are robust and will remain so for years to come.

Through the IC CAE program, we're committed to enhancing students' knowledge of the IC and guiding them as they develop the critical skills for the national security mission.

And, as I'm sure you emphasize to the students in this program, if they have a security clearance, their future is limitless. They can move between jobs, agencies, and roles during an IC career.

PERSONAL JOURNEY

While not at an IC CAE, my own journey to a career in national security began when I attended George Washington University as an undergraduate and studied international affairs.

I hadn't planned on working in the Intelligence Community, but a college internship opportunity at the Defense Intelligence Agency got me interested in pursuing an intelligence career.

I served for eleven years as an intelligence officer at DIA, where I held a number of senior analytic and management positions across the counterterrorism, counterintelligence, and counterespionage portfolios.

Along the way, I had many mentors who helped me grow and learn, and also helped me find opportunities and career paths that I may not have otherwise considered. People who helped equip me for the twists and turns that lay ahead and mentors who helped make connections, including working at the White House on the staff of the National Security Council before assuming my current post at NCSC.

I use my personal journey only as an example of the opportunities available to students who consider a path in intelligence and a testament to the role mentors – such as those through IC CAE – can have in shaping the next generation.

GLOBAL CI TRENDS OVERVIEW

Shaping the next generation and equipping them for the challenges ahead is so important because the landscape we face will only become increasingly complex.

Today, when we describe the counterintelligence threat landscape it can be summed up as … more, more, and more.

More adversaries: First, 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, the PRC, 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. They are no longer just targeting government secrets, but virtually every sector of our economy – including universities -- to acquire technology, data, and talent to advance their interests.

- **More data**: One need only consider the example of data and how important it has become. 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.

More attack vectors: To add to that, 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 scientific collaboration, mergers, acquisitions, investments, and joint ventures. They're using legitimate 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 one another, enhancing their skills, expanding their geographic reach, and magnifying the threat to the United States.

HOW THESE CI THREATS RELATE TO YOU

The reality is that this is not just a fight your students will enter when they join the workforce. Today, institutions like yours --because you are an IC CAE -- are a unique target of foreign intelligence services.

Transnational Repression on US Campuses: In recent years, we have seen transnational repression occurring on college campuses where repressive foreign nations and their proxies target foreign students on U.S. campuses who dare to speak out about abuses by their home governments. These students are being targeted for merely exercising their fundamental rights to free speech in America.

For example, the PRC government closely monitors the speech and behavior of Chinese students on US campuses. Beijing insists that its citizens at home and abroad conform to the views and ideology of the Chinese Communist Party. Those students here who don't conform to these mandates risk being targeted for harassment and their relatives in China may suffer retribution.

Just last month, a Chinese student at Berklee College of Music in Boston was convicted of stalking and threatening a fellow Chinese student who posted fliers on campus in support of democracy in China. The perpetrator threatened to chop off the victim's hands and alert the security services in China about this activity so they would target the victim's family in China.

These types of threats are not idle. A few years ago, a Chinese graduate student at Purdue University who spoke out about lack of freedoms in China was harassed by other Chinese students and his parents in China were visited and threatened by PRC security services. To his credit, the President of Purdue issued a letter in 2021 condemning tactics used to censor this victim on campus

Targeting Students for Potential Recruitment: We also see foreign governments exploiting the U.S. academic environment to collect information on fellow students or professors who may be seeking positions in the Intelligence Community or other U.S. Government agencies.

Last year, the Justice Department announced charges against Sergey Cherkasov, a Russian intelligence operative who posed as a Brazilian graduate student at Johns Hopkins University. Many students from Hopkins go on to serve in the U.S. government.

Cherkasov was tasked by his Russian handlers with making connections in D.C. and collecting information on his fellow students, professors, and others in think tanks and even officials in the current Administration. After his time at Hopkins, Cherkasov tried to get a position at the International Criminal Court at The Hague. These are the types of things your students need to be thinking about.

Targeting Emerging Technology, Research & Talent: Another huge problem involves foreign targeting of scientific research that goes on at academic institutions. This is a threat we see taking place routinely across the country.

Much of the research behind emerging technologies like AI and quantum is happening at U.S. academic institutions. Our adversaries are laser-focused on the economic and military benefits of these technologies, and they seek to acquire the research, innovation, and talent behind them.

Some nations have enacted comprehensive national strategies to achieve leadership in these technologies. Russia and other nations target these sectors to advance their own programs. But nobody goes after them like the PRC.

I want to emphasize that I'm speaking about the PRC's government, and not the Chinese people generally and not Chinese Americans, who are often victimized by the PRC.

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

Through national industrial plans like Made in China 2025 and the 14th Five Year Plan, the PRC has made clear it seeks to achieve global dominance in many of these technologies in the near future. China's national plans have become roadmaps for PRC theft across the U.S.

Unfortunately, they use every tool in the toolkit to get what they want. They may recruit an insider, use a cyber intrusion, forge a scientific collaboration, make an investment, recruit top talent, or do some combination of all of those things, to get the technology they want.

The bottom line is, the stakes couldn't be greater with respect to the global competition in emerging technologies. Authoritarian nations that lead the way in areas like AI, quantum computing, and synthetic biology will have the power to shape all of our futures. So, your students benefit not just from the great power competition at stake, but also the tactics that may already be at their doorstep.

RESEARCH TARGETING TACTICS

We see many tactics being used to target research at academic institutions, but let speak just about a few

- Talent Recruitment and Placement Programs
- Scientific Collaboration
- Cyber and Social Media Deception
- Foreign Student/Scientist Exchange Programs
- Professional Conferences

I'll just touch on three of them briefly, starting with talent poaching & recruitment:

Talent Poaching/Recruitment We continue to see threat actors aggressively poaching experts in AI, semiconductor, quantum, and other technologies from our research ecosystem for their own national development programs.

Increasingly, the competition for global technology is a competition for talent. Adversaries understand that acquiring top talent can be just as good as acquiring the technology itself. While it may be legal for them to hire America's best and brightest, the loss to our country is grave.

Threat actors play on a number of motivations in these recruitment pitches -- often offering lucrative salaries, perks, grants, awards, or scholarships.

For example, just last month, a renowned biologist and researcher at a U.S. scientific agency received an email from the China Overseas Outstanding Scientists Fund inviting the biologist to apply for a position in the PRC in the life sciences. The email offered the biologist a salary of up to $280,000, a housing subsidy, as well as priority school admission for children. Thankfully, the biologist self-reported the approach and did not respond to the job pitch.

In Taiwan—where there are laws against PRC talent poaching—there have been repeated crackdowns on PRC talent recruitment activities. Last year, Taiwan announced raids on nine local firms that were illegally poaching high-tech talent from Taiwan to help Mainland China with dynamic random-access memory (DRAM) and artificial intelligence (AI) chips.

Foreign Research Collaboration We also see threat actors leveraging research partnerships and collaboration to acquire information.

In one recent example, an adjunct professor at a U.S. university who is affiliated with a U.S. scientific agency received a request by a graduate student overseas to work collaboratively to develop next-generation quantum system theories that solve quantum problems.

Upon further examination, it turned out the overseas graduate student had received funding for this effort from a foreign adversarial government and was a student at a university affiliated with that nation's military. In addition, the specific research the graduate student wanted to work on was a match for a top collection priority by that foreign military.

We understand collaboration is essential for the U.S. research enterprise, but we want researchers to know who they're partnering with and understand this is an avenue that threat actors exploit.

Deception on Social Media / Networking /Job Platforms. Our adversaries are also particularly adept in using deception on social media, professional networking sites, and other job-focused platforms to target people for information gathering or recruitment. This includes targeting people in the U.S. academic community.

The PRC has used fake profiles on LinkedIn for years to target tens of thousands of people worldwide. In October, Britain announced that PRC operatives had targeted more than 20,000 Britons via fake profiles on LinkedIn. And they are not the only ones -- Russia and North Korea also use these techniques.

They often pose online as headhunting companies or someone with enticing career opportunities. They may 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.

For promising targets, they may offer paid trips abroad meetings or presentations at foreign universities. Once abroad, the target can be compromised and pressured to turn over more information.

Everyone with access to sensitive or proprietary data should be careful about what they post on social media – specifically about their clearance (if you have one), work, and contacts, as it could draw attention from adversaries or criminals.

BALANCING COLLABORATION WITH SECURITY

I've spelled out a lot of threats to the research enterprise here. The purpose of raising these issues is not to stifle research or reduce scientific collaboration, which helps fuel innovation across this country.

Rather, we want to help the research enterprise collaborate securely and with its eyes wide open. We seek to promote a U.S. research ecosystem that emphasizes collaboration, openness, integrity—*and security*—all of which facilitate innovation.

Not only is an informed, empowered U.S. scientific community best positioned to assess emerging technologies and their applications—it's also best positioned to design measures to guard against the potential misuse, theft or exploitation of these technologies.

We also want to emphasize the shared responsibility of the U.S. Government and the scientific community to protect research and innovation. Ultimately, we seek to develop a culture of security awareness. And we want your students, no matter where they end up to take that security mindset with them.

We would like to see an evolution from a "do no harm" mentality to a more explicit "not on my watch" mentality when it comes to protecting our research and technology.

MITIGATION RESOURCES

So how can we mitigate these threats?

NCSC and our partners have worked hard to provide the research community with tools they can use to develop safeguards that cater to their needs. We want to empower these communities to make security-informed decisions by providing information on risks and mitigation.

Enterprise Risk Mitigation Blueprint. Last October, NCSC disseminated a new resource on this issue called "Enterprise Risk Mitigation Blueprint for Non-Intelligence Agencies." It can be found on our website at **NCSC.gov** in the "Safeguarding Our Future" section.

While this document is geared primarily to federal agencies, all organizations should find it useful as well. Countering foreign threats requires an integrated approach across an organization to ensure both human and technical threats are addressed in a coordinated, holistic manner.

Safeguarding Science. Another resource I'd like to bring to your attention is our "Safeguarding Science" webpage at **www.ncsc.gov** This is essentially a one-stop-shop to access best practices related to research security.

In creating this toolkit, we partnered with scientific and research organizations across the government, as well as the academic community. Our partners for this effort include the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), the Department of Health and Human Services, and other agencies.

In short, these are research security tools developed ***by*** the scientific community ***for*** the scientific community.

Among other things, the website houses last week's guidance from the Office of White House of Science and Technology (OSTP) on foreign talent recruitment plans and a common form for those at federal research funding agencies to report potential conflicts of interest.

The Safeguarding Science site also houses all the latest research security materials from the National Science Foundation. There are also academic security resources, as well as information on CI, physical security, personnel security, supply chain risks and insider risks. The site also includes NIST's Research Security Framework, which was released in August 2023 to safeguard international science while mitigating risk to the integrity of the open collaborative environment.

Since this toolkit was launched over a year ago, it's been cited as a key resource by the White House Office of Science and Technology Policy, Stanford University, Caltech University, RAND Corporation, and other entities.

Researchers have let us know they're pleased this is not a government compliance program requiring them to fill out paperwork, nor is it a law enforcement or investigative effort that could result in fines or prosecutions.

Digital Wall of Spies – I spent some time talking about how the CI landscape has changed, but the history of the CI community is often one that tracks side-by-side with geopolitical conflict and national security crises today. Yet that rich history often remains in the shadows.

As you build your course schedule, I encourage you to consider building a CI course, expanding your students' view of the work the CI community does and how important it will be in the decades to come.

A number of years ago, we began building a Digital Wall of Spies to tell the story of counterespionage to the nation. It's already being used as a resource for classes and I encourage your students to check it out if they have not yet done so.

CONCLUSION

In closing, I know I've painted a sobering threat environment picture. The more, more, more nature of the CI threat landscape is our reality in 2024, and that landscape will likely become more complex in the years to come.

But the future need not be bleak. It can also be bright.

As IC CAE institutions, you hold the key to raising the next generation, to building CI into their course work, to encouraging them to think about the CI implications of their work, and to equip them no matter whether they come to the IC or industry – to protect our nation from the adversaries that seek to undermine it.

Thank you for inviting me to participate in the summit, and I look forward to your questions.