CYSE 200T – ODU FBI Presentation

Chadwick Bennett
February 23, 2026
Professor Duvall

Today's presentation by Julia Nickel, an FBI Intelligence Analyst, was very informative. She discussed how cyber threats are real, strategic, and tied to national security. Among the topics she discussed were:

1. How the FBI approaches an investigation
2. How cyber adversaries approach network intrusion
3. Intrusion by foreign nations, including China, Russia, North Korea, and Iran
4. Employment opportunities, information, and requirements for working with the FBI

Three of the things that most resonated with me include **China's infiltration into the United States infrastructure, the US top adversaries, and FBI employment.**

1. China's infiltration into the United States

I was surprised to hear that China had infiltrated the US infrastructure, including its power grids and water facilities. It was difficult to believe that, first, China was able to do that, but more importantly, that no one discovered it until October 2025. She discussed two investigative processes: how the FBI approaches an investigation and how cyber adversaries approach network intrusion. China's intrusion felt more aligned with a network intrusion. There were six intrusion steps:

1. Recon (reconnaissance)
2. Intel comparison
3. Establish a Hold
4. Elevate access

5. Cause chaos
6. Gather more intel

Why is this Important?

This meant that China could have weaponized this access by collecting enough information and "establishing a HOLD," to disrupt the US infrastructure, including communications, military, financial, hospitals, and business operations. It meant that they got through our defenses and could have threatened our national security, daily life, and impacted our economy, and we didn't have a clue.

Top US Adversaries

Nickel spoke about the four primary US adversaries, China, Russia, North Korea, and Iran. I wondered if these countries were discussed because they were always in the media, or if there were other equally important countries that we normally don't hear about, but should be concerned about.

Why is this Important?

Cybersecurity and cyberwar discuss nation-states as actors. Countries that want to bring harm to other nations using cyberwarfare. But nowadays, anyone can be an actor, and anyone can inflict pain, threat, or damage on anyone else or on a nation. It is important to know who or what actors are out there lurking to cause disruption. In a cyber attack, things happen at a much faster rate than traditional warfare. A slow response can have more devastating outcomes.

FBI employment

Nickel shared information about FBI internships, accessing the FBI employment website, and the need to submit applications by March 5, 2026, for employment opportunities in 2027, because a Top Secret clearance would be required, and it takes a year to process the clearance. She also stated that to maintain the Top Secret clearance, one has to work 16 hours/month during the academic year.

Why is this Important?

I am currently enrolled in ODU's cybersecurity program. I am also serving in the VA National Guard and participating in ODU's ROTC program. I had plans on applying for internships in the Summer of 2027. This was great information for me to investigate and possibly submit an application or get the process started before missing critical deadlines.

Conclusion

This presentation reinforced that there are constant ongoing threats greater than cyberwarfare that could greatly impact our lives beyond computers. There is so much discussion about AI, cybersecurity, and cyberwarfare that we have easily taking our eyes off other threats like China's infiltration of the US infrastructure. We are more vulnerable to our nation-state adversaries, but we are also very vulnerable to other actors. Finally, the information on FBI employment and the need to take action a year in advance was great intel that I can research and possibly take action on now.