Extract from "The FBI and the National Security Threat Landscape: The Next Paradigm Shift"

Christopher Wray, Director, Federal Bureau of Investigation

Remarks prepared for delivery

Council on Foreign Relations, Washington, D.C., 26 April 2019

Changing Threat Landscape

The nature of the threats we face is evolving—criminal and terrorist threats are morphing beyond traditional actors and tactics. We still have to worry about an al Qaeda cell planning a large-scale attack.

But we also now have to worry about homegrown violent extremists who are radicalizing in the shadows. These folks aren't targeting the airport or the power plant. They're targeting schools, sidewalks, landmarks, concerts, and shopping malls, with anything they can get their hands on, and often things they can get their hands on pretty easily—knives, guns, cars, and primitive IEDs [improvised explosive devices]. They're moving from radicalization to attack in weeks or even days, not years, online and in encrypted messaging platforms, not a camp or a cave.

On the cyber front, we're seeing hack after hack, and breach after breach. And we're seeing more and more what we call a "blended threat," where cyber and espionage merge together in all kinds of new ways.

We still confront traditional espionage threats, with dead drops and covers. But economic espionage dominates our counterintelligence program.

More than ever, the adversary's targets are our nation's assets—our information and ideas, our innovation, our research and development, our technology. And no country poses a broader, more severe intelligence collection threat than China.

China has pioneered a societal approach to stealing innovation any way it can, from a wide array of businesses, universities, and organizations. They're doing this through Chinese intelligence services, through state-owned enterprises, through ostensibly private companies, through graduate students and researchers, and through a variety of actors working on behalf of China.

At the FBI, we have economic espionage investigations that almost invariably lead back to China in nearly all of our 56 field offices, and they span almost every industry or sector. The activity I'm talking about goes way beyond fair-market competition. It's illegal. It's a threat to our economic security. And by extension, it's a threat to our national security.

But it's more fundamental than that. This behavior violates the rule of law. It violates principles of fairness and integrity. And it violates our rules-based world order that has existed since the end of World War II.

Put plainly, China seems determined to steal its way up the economic ladder, at our expense. To be clear, the United States is by no means their only target. They're strategic in their approach—they actually have a formal plan, set out in five-year increments, to achieve dominance in critical areas.

To get there, they're using an expanding set of non-traditional methods—both lawful and unlawful—weaving together things like foreign investment and corporate acquisitions with cyber intrusions and supply chain threats.

Federal Bureau of Investigation (FBI) Director Christopher Wray discusses the national security threat landscape 26 April 2019 during an interview with Council on Foreign Relations President Richard Haass in Washington, D.C. (Photo courtesy of the FBI)

The Chinese government is taking the long view here—and that's an understatement. They've made the long view an art form. They're calculating. They're focused. They're patient. And they're persistent.

Overlaying all these threats is our ever-expanding use of technology. Next-generation telecommunication networks, like 5G, and the rise of artificial intelligence and machine learning. Cryptocurrencies, unmanned aerial systems, deep fakes—a lot of stuff I wasn't particularly focused on when I was in the private sector is suddenly blinking red right in front of me, in front of all of us.

And we grow more vulnerable in many ways by the day.

Taken together, these can be called generational threats that will shape our nation's future. They'll shape the world around us. And they'll determine where we stand and what we look like 10 years from now, 20 years from now, 50 years from now.

How We're Addressing the Threat

Our folks in the FBI are working their tails off every day to find and stop criminals, terrorists, and nation-state adversaries. We're using a broad set of techniques, from our traditional law enforcement authorities to our intelligence capabilities.

We've got task forces across the country, with partners from hundreds of local, state, and federal agencies. We've got task forces targeting everything from terrorism to violent crime to cybercrime to crimes against children to crime in Indian country—you name it.

We've got legal attaché offices stationed around the world to focus on joint investigations and information sharing.

We've got rapid response capabilities we can deploy at a moment's notice, for any kind of crime or national security crisis.

And on the nation-state adversary front, along with our partners, we've got a host of tools we can and will use, from criminal charges and civil injunctions to economic sanctions, entity listing, and visa revocations.

But we can't tackle all these threats on our own. We've got to figure out how to work together, particularly with all of you in the private sector. We need to focus even more on a whole-of-society approach. Because in many ways we confront whole-of-society threats.

To view the entire speech transcript, please visit https://www.fbi.gov/news/speeches/the-fbi-and-the-national-security-threat-landscape-the-next-paradigm-shift.