

FBI HAS ALMOST 20 CYBERS STATIONED AROUND THE WORLD


As part of cybersecurity awareness month, the FBI published this release about having almost 20 cybersecurity “Assistant Legal Attachés” around the world.

Another way we’re working to combat the cyber threat is by placing Bureau cyber experts in FBI legal attaché (legat) offices in strategic locations around the globe—a critical step because cyber threat actors can and do operate virtually anywhere in the world, crossing national and international borders with a few strokes of a keyboard to reach their victims.

Our experts are called cyber assistant legal attachés, or ALATs, and they work on a daily basis with law enforcement in host countries, sharing information, cooperating on investigations, and enhancing our relationships overall. Sometimes, they even work in the same physical space alongside their foreign counterparts.

The cyber ALAT program began in 2011, when several FBI Cyber Division personnel were deployed to a handful of legat offices to address significant cyber threats in those regions impacting U.S. interests and FBI investigations.

Five years later, there are eight permanent cyber ALAT positions—two in London and one each Bucharest, Romania; Canberra, Australia; The Hague, Netherlands; Tallinn, Estonia; Kyiv, Ukraine; and Ottawa, Canada. And currently, the Bureau maintains nearly a dozen temporary duty (TDY) cyber ALAT positions—their locations determined by



the cyber threat environment and the host nation's capabilities in working with the FBI in identifying, disrupting, and dismantling cyber threat actors and organizations.

I get the value of this program. The investigations into some of the most disruptive cyberattackers require a lot of resources, and surely those resources are better spent if they're working closely together.

But it does raise some questions. If an FBI Agent is working overseas and deploys an exotic technique there, is it bound by US law, the law of the host country, or by EO 12333? And if that technique ends up nabbing US defendants, do those defendants learn in discovery that the evidence came from an FBI Agent partnering with foreign law enforcement (or spooks) overseas? Or does this just get laundered with the protection DOJ provides foreign evidence.

All these cyber tools disembodied from a legal jurisdiction may be necessary, but it'd be nice to know what, if any, laws they operate under.