


# What Is the Point of These Nation-State Indictments?

 lawfareblog.com/what-point-these-nation-state-indictments

February 8, 2021



Skyline of Pittsburgh, Pennsylvania. (Pixabay, <https://tinyurl.com/1aki1c38>; <https://pixabay.com/service/license/>)

When the U.S. Department of Justice unsealed the indictment in 2020 that charged six military intelligence officers in Russia’s GRU with some of the most infamous cyber crimes on record, it did so with great fanfare. Leading off the 30-minute press conference in Washington on Oct. 19, John Demers, the assistant attorney general for national security, called the crimes “the most disruptive and destructive series of computer attacks ever attributed to a single group.” Demers wasn’t being hyperbolic. NotPetya, the most notorious attack engineered by this group, known as Sandworm, victimized dozens of companies and millions of people and caused an estimated \$10 billion in damages.

The indictment received mixed reviews. Writing in Lawfare, Harvard law professor (and Lawfare co-founder) Jack Goldsmith was highly critical of both the document and the timing, noting that the rollout occurred just two weeks before the presidential election. “What is the point?” Goldsmith asked before answering his own question. “In a word: attribution.” He

noted that government officials had asserted that the indictment was a warning to would-be hackers that the government can gather undeniable evidence proving the attack, and it highlighted the government's ability to identify the perpetrators.

Goldsmith was not impressed. "This warning and highlight are not news," he continued, "at least not to the sponsors of the attacks. The United States has for six years been playing up its extraordinary intelligence capacity to attribute malicious cyber operations. And for six years the attacks have grown worse." (He wrote this two months before Russia's SolarWinds hack made even bigger headlines, raising the most serious questions yet about the country's capacity to sniff out cyber threats.)

Goldsmith couldn't understand why Demers and the others who took their turns at the podium were congratulating themselves. "None of my criticism is meant to minimize the horror of the Russian actions," he emphasized. "But naming and shaming is not much accountability. And trumpeting that fact is puzzling." Especially right before the presidential election, when the government should be assuring citizens that voting will be safe and secure. Instead, Goldsmith suggested, the recitation of these crimes could well have the opposite effect.

Many viewers of the press conference may have come away reassured by the "gotcha" speech they heard from Demers. But Goldsmith had a point. Putting aside the timing of the announcement, it does seem worth asking the deeper question. What are these indictments accomplishing? The United States does not have an extradition treaty with Russia. And these guys from the GRU are not exactly going to bring their families to Disney World; if they did, they'd find themselves in handcuffs long before they made it to Space Mountain.

When you look at the tangible results of these nation-state indictments, it's hard to see a lot of wins. None of the men whose names and photographs have graced their pages has landed in prison. Or even faced trial. That's a lot of time and money spent for words in a legal document.

But amid all of the doubts, the nation-state hacking indictments have achieved real progress. Investigators have uncovered a great deal of information about this netherworld. They have learned how to build cases, and how to cooperate with their counterparts in far-flung locations. Countries that have seen enough of these crimes have worked together to find common solutions. Some of these collaborations have surprised even the participants—and might surprise their critics, if they were better known.

There were similar doubts when the Justice Department rolled out the first of these indictments six years ago. The focus then was China, and the alleged crime was economic espionage. There had been years of complaints about this sort of thing. But back then, it was left to security companies like Mandiant (now part of FireEye) to present evidence of cyber crimes and attribute them publicly (which Mandiant did in China's case in 2013). Before the Justice Department decided to pursue an indictment against five members of the People's

Liberation Army (PLA), President Obama's cautious nature seemed to align with the widely perceived futility of attempting legal action against agents of the Chinese government. But behind the scenes, under pressure from the many U.S. companies that claimed they'd been victimized by Chinese attacks, government officials were confronting their counterparts in China with evidence of crimes. And they were drawing a distinction between spying, which they acknowledged that all nations do, and theft. When the evidence they presented to China was repeatedly rejected out of hand, the administration finally decided to act.

The indictment was signed by David Hickton, then-U.S. attorney for the Western District of Pennsylvania, who spearheaded the initiative. The FBI's Pittsburgh field office had gathered highly detailed evidence that PLA officers had stolen proprietary information from, among others, U.S. Steel and the nuclear power firm Westinghouse. Hickton took it to a grand jury and obtained a sealed indictment. After months of back and forth between Justice and the State Department, which opposed legal action against the PLA, the indictment was finally unsealed in May 2014.

At the time, Goldsmith wrote a measured response. He had reservations. Everyone seemed to have some. Commentary and news articles alike acknowledged the obvious: There was virtually no chance anyone would ever be tried on these charges. But Goldsmith did not dismiss the indictments as political theater. "Until yesterday," Goldsmith wrote, "the [U.S. government] complaints against China's cyber-snooping were nothing but talk.... But yesterday's step clearly (and predictably, and thus purposefully) offended the Chinese in a way that prior talk did not, and to that extent it shows that the [U.S. government] is somewhat more serious about this issue, and might retaliate further regardless of the costs to itself." A Wall Street Journal editorial was less charitable. "The U.S. should respond with its own cyber battle plan that attacks Chinese targets and forces China to play defense rather than devote all of its resources to hacking U.S. targets." The editorial concluded: "We can say with certainty that an indictment of five junior PLA hackers will be no deterrent at all."

As it turned out, the editorial was wrong. The indictment may not have accomplished a great deal by itself, but it was part of a strategy the Obama administration used to pressure China to change course. And change it did. As New York Times reporter David Sanger wrote in his book "The Perfect Weapon," China replied by insisting that the indictment contained "fabricated facts," a pretty flimsy response. Then-Attorney General Eric Holder's rejoinder, according to Sanger, was: "If we fabricated all of this, then come over to Pittsburgh and embarrass us by forcing us to put up or shut up, and we'll put up." The leverage that the administration needed to press its case was President Xi Jinping's first state visit to Washington in September 2015. Obama's team was threatening to impose sanctions on China for cyberattacks, including the PLA's. Xi was determined to avoid anything that would blemish his visit. On the eve of his trip, Xi sent an advance delegation to Washington to negotiate. Before China's president returned home, he and Obama announced an agreement that their governments would not, in Obama's words, "conduct or knowingly

support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage.” And two months later, leaders of the G-20 all committed to abide by the same agreement.

So, was the PLA indictment a game-changer? Not exactly. There was no way to enforce it. And it didn't end China's hacking. Yet the Justice Department continued issuing these indictments and expanded the targets to include members of Iran's Islamic Revolutionary Guard Corps, for its alleged role in a series of distributed denial-of-service attacks on U.S. financial institutions, and North Korean computer programmer Park Jin Hyok, for his alleged involvement in a host of attacks, including those on Sony Pictures Entertainment after the studio released "The Interview." And before the latest GRU indictment, Special Counsel Robert Mueller indicted a dozen members of that organization in 2018 for attacks that sought to influence the 2016 presidential election. Some of these indictments were accompanied by sanctions, but from the look of things, none has matched the success of the first.

So why expend the resources? Because these indictments have accomplished things that shouldn't be taken for granted. They may not be dramatic, but they're foundational. Attributing an attack is the first step in holding a nation-state accountable—if nowhere else, then in the court of public opinion. For too long the U.S. government preferred to remain mum after a cyberattack, which suggested it was too ashamed to acknowledge the attack, too baffled to identify the source or too afraid to attribute it. Laying out the evidence shifts the blame from victim to perpetrator. It paves the way for sanctions. And it gives the world a close look at the dangers in a legally rigorous form that cannot easily be dismissed as “fabricated facts.”

If anything, this seems more important today than it did in 2014. The past four years have been a time of “alternative facts.” A large segment of the U.S. population still believes arguments about last year's election that were thrown out of scores of courts for lack of evidence—any evidence. It's never been more important to support the rule of law. And if there was ever a time when the U.S. had reason to hold Russia to account—after what amounts to a four-year pass—this is it. That's one reason the Sandworm indictment was surprising and noteworthy. Like the first indictment brought against China, this one also came from the U.S. attorney in Pittsburgh—this time, Republican appointee Scott Brady. It focused on a broad range of attacks that began in 2015 and extended into 2019. They included some in the Western District of Pennsylvania, but a big difference from previous indictments is that nearly all of them occurred far from U.S. shores.

Writing in Slate after the unsealing of the Sandworm indictment, Josephine Wolff was surprised at “the U.S. willingness to use the full force of its own legal system to censure Russia for these attacks on non-U.S. targets.” A professor at Tufts University's Fletcher School of Law and Diplomacy, Wolff saw this indictment as “a signal not just to Russia but also to the rest of the world that the U.S. government regards online attacks on Ukrainian

infrastructure, South Korean events, French politicians, Georgian media outlets, and U.K. government ministries as deserving of the same response as attacks on U.S. companies and elections.”

Like the PLA indictment, this one was part of a strategy. It was preceded by a monthslong effort to build a coalition of countries to call out Russia. That initiative achieved liftoff in February 2020, when the U.S. and the other “Five Eyes” countries, along with most of the EU, publicly attributed Russia’s alleged attacks on the country of Georgia. At the time, the effort was praised for the show of solidarity, and there were calls for more collective action of this kind. But it was also criticized for the absence of hard evidence—another indication that indictments are important. That evidence, by the way, was delivered eight months later in the Sandworm indictment, which added considerable heft to the package. It wasn’t simply another example of the U.S. acting unilaterally to make some sort of statement. Instead of one voice, there was a chorus. And a chorus of voices naming and shaming has a greater chance of deterring bad behavior than naming and shaming delivered by a soloist.

There’s another piece of the equation. Some cyber criminals in Eastern Europe work in both the public and private sectors. They are players in organized crime. And their private work sometimes bleeds into hacking they do for nation-states—specifically Russia. And sometimes their criminal infrastructures are used by both of these enterprises. An early example popped up in an indictment unsealed a week after that 2014 PLA indictment. This one involved a Russian named Evgeniy Bogachev, who in many respects was way ahead of his time. He was operating what was known as the GameOver Zeus Botnet, a global network of an estimated 1 million computers infected with malware. Bogachev and his cronies used this vast infrastructure to steal companies’ banking credentials and wire themselves money from company bank accounts. They employed citizens who were not connected to their gang to be money mules tasked (some unwittingly) with laundering the stolen funds. He also launched ransomware attacks years before they were a runaway hit with criminals. At the time of the indictment, Bogachev and his confederates were believed to have stolen more than \$100 million.

He’s never been caught. He doesn’t seem to stray from Russia. His victims are mostly companies from the West. And he’s found ways to spy for his country, which undoubtedly adds to his patina of untouchability. But if Bogachev was beyond the reach of the law, his criminal infrastructure was not. The triumph of this case wasn’t that an indictment was unsealed. It was that law enforcement was able to take down his giant botnet. How? Just as the criminals were able to wreak havoc through an international confederation, law enforcement succeeded by marshalling their own international gang. The press release celebrating the takedown credited the work of officers in no fewer than a dozen countries.

Paul Rosenzweig wrote about the case in Lawfare. Rosenzweig was impressed by the broad cooperation—most surprisingly Ukraine’s. Authorities there seized servers in contested territory: “a remarkable commitment from an unstable government,” Rosenzweig wrote. “As with the Chinese indictment [from the previous week], this case was brought in Pittsburgh,”

he noted, “which is an odd location to choose. Apparently, the office is developing an expertise in cyber crime.” He concluded by complimenting “an effective use of law enforcement” and an “aggressive use of criminal law” that together signaled “that the U.S. is willing to take steps in defending its networks that it has heretofore been a bit reluctant to take.”

Equally remarkable, in 2016 the U.S. attorney’s office in Pittsburgh obtained a sealed indictment that alleged a Bulgarian man was part of a gang that bore some resemblance to Bogachev’s. Its victims were small- to medium-size businesses in the U.S. and Western Europe. The Bulgarian was arrested because he was the only one of the group who lived in a country that had an extradition treaty with the United States, and he was promptly sent to Pittsburgh. One of the men was based in Ukraine, where he ran a “bulletproof” hosting service called Avalanche, which registered malicious domains for cyber criminals and hosted their executable malware files on its servers. The investigation of this criminal enterprise continued until 2019, when the U.S. attorney’s office unsealed an indictment that charged 10 men with a conspiracy to steal funds using Avalanche and GozNym malware. None of the men worked directly for a nation-state (as far as could be learned), but five of them were in Russia. The others were in Ukraine, Georgia and Moldova. It looked like just another name-and-shame indictment. That familiar question surfaced again: What was the point?

But the prosecutors and FBI agents in Pittsburgh were not willing to let it go. They flew to The Hague to meet with their counterparts from countries where victim companies were located and where the gang members were based (except Russia). And they agreed to work together to bring as many of the criminals to justice as they could—no matter where that was and no matter who received credit. Germany was a major player. Europol and Eurojust were deeply involved. The five in Russia were beyond their grasp. But much to the surprise of the many naysayers, the others were not. Three, including the ringleader, were arrested in Georgia. One of the FBI agents in Pittsburgh, who helped work the case, testified during the Georgian trial by video linkup. All three were convicted, and the ringleader was sentenced to seven years in prison. The Avalanche administrator was arrested in Ukraine. He escaped, only to be rearrested. Then a judge inexplicably released him pending trial, and he disappeared. The Bulgarian pleaded guilty in Pittsburgh and was sentenced to time served (about three years).

Did these cases transform the landscape? Hardly. There’s no shortage of cyber criminals in Eastern Europe. The downfall of Avalanche and the conviction of four men didn’t put a dent in their ranks. But it was an important step. The Sandworm indictment in October that focused on global attacks was impressive. But putting in the time and effort to develop evidence and relationships with cops and prosecutors far away—and trusting that they would succeed, while knowing that they would get the credit if they did—was no small thing. It’s how you build teams. It’s how you support the rule of law in places that have less experience with it.

Maybe it's time to stop asking that question about indictments. Here's the bottom line. If there's ever going to be a real chance in the legal realm to make a dent on cyberattacks—whether the perpetrators are nation-states, organized gangs or individuals—the good guys will have to show they know how to collaborate at least as well as the bad guys. Some of them seem to have gotten that message.