FBI'S FANCY BEAR CYBER STRUCTURE

Back in July, I noted this passage in the latest DOJ IG report on FBI's cyber prioritization.

> According to the FBI, computer intrusion matters Involving national security are the highest priority matters investigated by the FBI Cyber Division. National security computer intrusion matters are intrusions or attempted intrusions into any computer or information system that may compromise the confidentiality, integrity, or availability of critical infrastructure data, components, or systems (e.g., cyber national security incidents or threats to the national Information infrastructure) by or on behalf of a foreign power, or an agent of a to include designated international terrorist groups. [half paragraph redacted]
>
> In FY 2015, to ensure t hat the highest ranked threats are efficiently investigated, the Cyber Division implemented its Cyber Threat Team (CIT) model. A CTT focuses on the investigation of and operations against a specific national security threat. Each CTT is comprised of lead field office, called a Strategic Threat Execution office, up to five field offices assisting in specific aspects of the threat called Tactical Threat Execution offices, and a Cyber Division headquarters threat manager. The CTT bears the responsibility for managing the strategy, operations, and intelligence for its assigned threat. [half paragraph redacted]
>
> The intention of the Cyber Division's err model is to facilitate the

> allocation of resources to cyber national security threats, increase efficiency in addressing those threats, and facilitate the development of subject matter expertise within various field offices. Additionally, the CTT model is intended to enable each field office to focus on specific, assigned threats, helping to prevent the previous diffusion of efforts wherein multiple field offices were working the same cyber threat and not coordinating efforts. Prior to the implementation of the err, such overlapping investigations were a great challenge for the FBI. While its field offices each have a territory for which they are responsible, cyber threats are not restricted by geographical boundaries, so a territorial model proved ineffective. Lastly, the err model is intended to assist the FBI in prioritizing and properly allocating resources to each field office based on the threats on which they are assigned to work.
>
> The Cyber Division organizes its headquarters national security intrusion threat operational units geographically, including sections responsible for identifying, pursuing, and defeating cyber adversaries emanating from Asia, Eurasia, and Middle East/Africa. Such geographic delineations of responsibility do not present the same problems at Cyber Division Headquarters, since responsibility for the threats is based on their point or area of origin, and not the multiple U.S. jurisdictions where they might have an impact. The threat operational units coordinate with the errs and with units of the Cyber Intelligence Section, which also are geographically organized and provide actionable intelligence information.

In other words, at both the field office level and at the national level, the FBI's cyber agents have reorganized around the geography of the threat rather than the geography of the target.

Jim Comey elaborated on this reorganization in a speech on cyber (and back dooring encryption) last week.

> The challenge we face today, with a threat that comes at us at the speed of light from anywhere in the world, is that physical place isn't such a meaningful way to assign work any longer. Where did "it" happen when you're talking about an intrusion that's coming out of the other side of the globe, aimed at multiple enterprises either simultaneously or in sequence? That "it" is different than it ever was before.
>
> So we've changed the way we're assigning work. We have now created a Cyber Threat Team model, where we assign the work in the FBI based on ability. Which field office has shown the chops to go after which slice of the threat we face—that stack? And then assign it there.
>
> This does two things for us. It allows us to put the work where the expertise is, and it creates a healthy competition inside the FBI. Everybody wants to be at the front of the list to own important threats that come at us. We assign, in the Cyber Threat Team model, a particular threat. *Let's imagine it's a particular threat that comes at us from a certain nation-state actor set. We assign that to the Little Rock Division because the Little Rock Division has demonstrated tremendous ability against that threat.*
>
> But we're not fools about important physical manifestations, because that

> threat is going to touch particular enterprises around the country. And the CEOs of those enterprises and their boards are going to want to know, “Has the FBI been here to talk to us? And what’s the nature of the investigation? And how is it going?” To make sure we accommodate that need, we’re going to allow up to four other offices to help the team that is assigned the threat in Little Rock. If a company is hit in Indianapolis, and one is hit in Seattle, and one is hit in Miami, those field offices will also be able to assist in the investigation, but the lead will be in Little Rock. Then, the air traffic control for all of that to make sure we are not duplicating effort, or sending confusing messages, will come from the Cyber Division at Headquarters.
>
> We’re trying this. We’ve been doing it now for about a year in a half. Seems to be working pretty well. It has set very, very healthy competition inside the FBI, which is good for us. But we’re confronting a challenge and a way of doing work that we’ve never seen before, so we’re eager to get feedback and then iterate as make sense. We want to be humble enough to understand that just as our world has been transformed in our lifetimes, the way in which we do our work is being transformed. We have to be open to changing when it makes sense.
>
> So the Cyber Threat Team model is at the core of our response. Also at the core of our response is a “fly team” of experts that we’ve put together that we call the CAT team—the Cyber Action Team. Just as in terrorism, we have pre-assigned pools of expertise that can jump on an airplane and go anywhere in the world in response to a terrorism threat, we’re building that, and have built, that same capability in respect

> to cyber, so that, if there is a particular intrusion—let's say Sony in Los Angeles—we have the talent, the agent talent, the analyst talent, the technical talent, that's already assigned to the Cyber Action Team that's ready to deploy at a moment's notice to literally fly to Los Angeles to support the investigation.

Comey had just defined "the stack" he refers to here as the priority of threats the FBI faces; nation-states, with China, Russia, Iran, and North Korea named, followed by multinational criminal syndicate, followed by "purveyors of ransomware," followed by hactivists, with terrorists (who Comey says aren't yet developing a hacking capability) last. This would suggest that this means no ransomware is perpetrated by multinational crime organizations, which would surprise me.

Now, I get the logic of such organization. Not only can network intrusions be launched from anywhere, but they usually hide where they're launched from. So geographical location, in this scheme, appears to be about holding corporate CEO hands (I guess they get different victim service from the FBI than the rest of us), not investigative venue.

But it also raises a few concerns for me.

Will devolution of cyber lead to more abuse of venue?

First, questions of venue for prosecution. We've already seen, with Weev, DOJ prosecuting a hacker (I'm not sure where Weev would be defined in this stack, because he wasn't doing it for political reasons) in an improper venue because of the nifty precedents there. With Playpen, we've got DOJ — before Rule 41 gets rewritten — hacking thousands based off one Eastern District of Virginia magistrate's warrant.

This dispersed focus would seem to encourage such legally problematic moves.

To the Fancy Bear watchers everything looks like a Fancy Bear

In addition, there's a potential problem with assigning cases by perceived perpetrator, one that replicates a problem in the private contracting world, where contractors routinely hype the threat of the day (which today is Russia, but which a few years ago was China) because it drove sales.

That is, at some level, FBI appears to be assigning cases based on preliminary evidence to specific CTTs. This seems potentially very problematic from an investigative standpoint, as it answers the question, "whodunnit," at the beginning of the process, not the end. And that particular CTT has an incentive to keep any big flashy case in its own hands, meaning they're going to be disinclined to see any other potential actors out there.

Moreover, if a case — say the DNC hack —that could involve multiple intrusions or actors with competing interests gets assigned to the group whose bureaucratic imperative requires it to be just one actor, it is far less likely they're even going to see the evidence that something more may be going on.

Again, this is just a potential problem, but it could be a very serious one, as it could reverse the investigative model that FBI has traditionally used.

FBI's 702 activities have been devolved as well and with that devolution undergo less oversight

Finally, this potentially exacerbates a concern I have with how FBI manages Section 702. The

most recent batch of Semiannual reports that came out show that more 702-related functions are devolving to FBI Field offices, with one redaction (see italics) suggesting there might be some role involving tasking going on at Field offices. And as this passage from the October 2014 report suggests, ODNI is not monitoring things as closely.

> During this reporting period, NSD continued to conduct minimization reviews at FBI field offices in order to review the retention and dissemination decisions made by FBI field office personnel with respect to Section 702-acquired data. As detailed in the attachments to the Attorney General's Section 707 Report, NSD conducted minimization reviews at sixteen FBI field offices between June 1, 2013, through November 30, 2013 and reviewed *[redacted]* involving Section 702-tasked facilities.
>
> ODNI participated in one of these reviews,10 and received written summaries regarding any issues discovered in the other reviews. (U//FOUO) NSD's review of field offices coincided with FBI's broadening of the use of Section 702-acquired data at these field offices. Although there were isolated instances of noncompliance with the FBI minimization procedures and/or FBI policy, NSD and ODNI found that overall agents understood and were properly applying the requirements of FBI policy and the minimization procedures.11
>
> 10 (U) ODNI joins NSD on these reviews when the FBI field offices are located in or within reasonable driving distance of the Washington, D.C. area (e.g., the Washington Field Office and the Baltimore Field Office). During this reporting period, ODNI joined NSD for

> the Baltimore Field Office review. ODNI plans to continue to accompany NSD during the minimization reviews of the FBI Washington and Baltimore field offices and is continuing to explore the feasibility of joining NSD on reviews of other FBI field offices.
>
> 11 (S//NF) NSD's review found only one instance where U.S. person information was not properly handled as required by the minimization procedures. Specifically, the agent improperly disseminated U.S. person information that did not meet the standard minimization procedures requirement. Although the information reasonably appeared to be foreign intelligence information, it did not seem to have met the requirement that such information shall not be disseminated in a manner that identifies a United States person unless such person's identity is necessary to understand foreign intelligence information or to assess its importance. In this case, upon NSD's review, the agent agreed that the disseminated U.S. person identity did not meet the above standard. NSD confirmed that the agent recalled the dissemination and re-issued the dissemination without identifying the U.S. person.

Along with some interesting new redactions in the boilerplate about FBI's roles in 702, the October 2014 and June 2015 report both include this paragraph:

> While prior Joint Assessments provided figures regarding the number of reports FBI had identified as containing minimized Section 702-acquired United States person information, in 2013 FBI transitioned much of its dissemination from FBI Headquarters to FBI field offices. NSD is conducting oversight

> reviews of FBI field offices use of these disseminations, but because every field office is not reviewed every six months, NSD no longer has comprehensive numbers on the number of disseminations of United States person information made by FBI. FBI does, however, report comparable information on an annual basis to Congress and the FISC pursuant to 50 U.S.C. §1881a(l)(3)(i).

Ummm. We know that the FBI's numbers on NSLs are bullshit — and FBI doesn't much care. And when asked about those inaccuracies, FBI told DOJ's IG,

> [T]he FBI told the OIG that while 100 percent accuracy can be a helpful goal, attempting to obtain 100 percent accuracy in the NSL subsystem would create an undue burden without providing corresponding benefits. The FBI also stated that it has taken steps to minimize error to the greatest extent possible.

I've even asked ODNI about FBI's funny NSL numbers, twice, and gotten this response:

> ¯_(□)_/¯

So we already know that the FBI's legally mandated reports to Congress on NSL numbers are bogus. Now we learn that FBI has devolved its 702 work to field offices which has led to the discontinuation of one of the key oversight mechanisms on their counting process: an outside check.

That seems like a potentially big oversight loophole.