THE THIN INDICTMENT AGAINST BEHZAD MESRI

I have long cautioned against DOJ's increasingly frequent practice of indicting hackers from other states as some kind of nation-state escalation. Once we normalize that practice, our own nation-state hackers risk a whole lot of new challenges in retaliation.

But at least for the prior cases, DOJ has shown evidence the substantiate its claims. When, in 2014, DOJ indicted some People's Liberation Army hackers for spying on the negotiations (and, in just one case, stealing IP) from US entities including the Steelworkers, the indictment described the subject lines of phishing emails, the dates malware was implanted, the file names, the computer hostnames, and the command and control domain names used.

When, in 2016, DOJ indicted some Iranians for DDOS attacks on some banks, the described what roles each hacker played, though, they did not substantiate the claim that the hacking groups, Mersad, "performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps."

The indictment against two FSB officers and two criminal hackers for pwning Yahoo earlier this year was remarkably detailed, going so far as describing communications between the two FSB officers. It provided a screenshot of the cookie manager used to access a Yahoo engineer's

account. It described a long list of victims both within and outside Russia. It listed the dates on which the hackers had shared passwords of victims and provided the transfer details for payments.

It is admittedly possible DOJ provided so many details because the two FSB officers had already been arrested for treason by the time of the indictment.

When, later this year, DOJ indicted Yu Pingan, who reportedly had a role in the OPM hack but who was indicted in conjunction with some compromises of defense contractors, it described the actual dates of compromise, named the exploit, tied Yu and his co-conspirators to domain names used in the hacks, listed those domain IPs, and then used intercepted communications to tie him to his co-conspirators.

Of course, with both Yu (who was picked up while he visited the US for a conference) and Yahoo defendant Karim Baratov who has since been extradited from Canada and appears to be cooperating), there will be an actual prosecution, which explains why DOJ included so much more detail.

But the indictment against Behzad Mesri, an Iranian DOJ today accused of hacking HBO, includes very little meaningful detail.

The indictment foregrounds, in the first paragraph, claims about Mesri's past ties to the Iranian state, though it never substantiates that claim.

> MESRI as a self-proclaimed expert in computer hacking techniques, and had worked on behalf of the Iranian military to conduct computer network attacks that targeted military systems, nuclear software systems, and Israeli infrastructure.

The actual details proving Mesri's role in the

the attack are far less detailed. While it provides the general timeline of the compromise (May through July), it doesn't show evidence it knows which accounts got compromised (though it does list the shows that got stolen). It also doesn't tie Mesri to the pseudonym, Mr. Smith, publicly used by the hackers who released HBO's files.

Significantly, the most detailed part of the indictment, which describes the extortion, repeatedly describes messages sent from an anonymous email, without tying those emails to Mesri beyond an introductory paragraph alleging he sent them. It asserts Mesri sent emails publicizing his acts — and includes the graphic he included, which made a nice graphic for mainstream reports of the indictment — but doesn't provide much detail of that, either.

None of that's to say DOJ doesn't have the evidence to support this indictment. It just says they seem to have no reason to present it. And why should they? Given that Mesri is almost certainly not going to be extradited, this case will never go to trial.

The thin details here support the reporting from WaPo that DOJ has been pushing prosecutors to unseal indictments in cases against Iranians to support bringing more pressure on the regime.

> [T]he HBO case is one of several that senior officials would like to unseal in coming weeks. The push to announce Iran-related cases has caused internal alarm,

> according to people familiar with the discussions, with some law enforcement officials fearing that senior Justice Department officials want to reveal the cases because the Trump administration wants Congress to impose new sanctions on Iran.
>
> A series of criminal cases could increase pressure on lawmakers to act, these people said.
>
> Asked about that report, [Acting SDNY US Attorney Joon] Kim did not give a direct answer, saying he decided to unseal the charges in the HBO hacking case before the story published. He did acknowledge the short amount of time it took to unseal the charges was unusual for such a case but said that was because of the FBI's exemplary investigative work.

It may be great investigative work. Perhaps, too, DOJ is just trying to hide any sources and methods that will never need to be disclosed in a trial. But treating this indictment any differently than any other one, particularly than ones that DOJ knows will have to face adversarial challenge, threatens to politicize claims that already carry the potential for international backlash.

By all means, let's pursue international hackers, and where they have real *current* ties to their state, lay out that tie. But don't turn hacking indictments into spectacle to serve larger political whims, because it will diminish the value of other DOJ claims on hacking.