REMEMBER WHEN WE ACCUSED IRAN OF HACKING?

I meant to mention this in my earlier post about David Sanger's StuxNet story, and this passage by Matthew Waxman reminded me.

> As I've argued elsewhere, it's likely that in many cyber-attack scenarios, *both* sides – the attacker and the attacked – will have great incentive to maintain very tight secrecy about it; among other reasons and aside from political considerations, the attacked will not want to disclose information about its vulnerabilities and responses. In light of the "secrecy and low visibility of some states' responsive actions [to cyber-attacks]… it will be difficult to develop consensus understandings even of the fact patterns on which states' legal claims and counterclaims are based, assuming those claims are leveled publicly at all." In writing this, I may have underestimated how much information might leak from the attacking side.

While he sources this information to the public comments of an Iranian general, Sanger suggests Iran has started its own cyberwar unit.

> Iran initially denied that its enrichment facilities had been hit by Stuxnet, then said it had found the worm and contained it. Last year, the nation announced that it had begun its own military cyberunit, and Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and

> Internet warfare." But there has been scant evidence that it has begun to strike back.

The thing is, while the US provided no detail to explain this claim, in February Treasury claimed that Iran's Ministry of Intelligence and Security participated with Hezbollah on some hacking projects.

> MOIS provides financial, material, or technological support for, or financial or other services to Hizballah, a terrorist organization designated under E.O. 13224. MOIS has participated in multiple joint projects with Hizballah in computer hacking.

I assume this is either an admission that Hezbollah has hit us or—perhaps more likely—Israel with attacks. (When I wrote this post, I wondered if the allegations that Hezbollah had hijacked Israeli drones—which quickly appeared to be Mossad sabotage instead—were the claimed hack.)

Whatever the basis for the claim, the US government, with a straight face, based part of its Iran sanctions on accusations that the mean old Persians have hacked … somebody.