THE STUXNET TEAM REUNION

On Thursday, DOJ had a big dog and pony show over the indictment of 7 Iranians in connection with cyberattacks on US banks and a small dam in suburban NY.

> A grand jury in the Southern District of New York indicted seven Iranian individuals who were employed by two Iran-based computer companies, ITSecTeam (ITSEC) and Mersad Company (MERSAD), that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps, on computer hacking charges related to their involvement in an extensive campaign of over 176 days of distributed denial of service (DDoS) attacks.
>
> Ahmad Fathi, 37; Hamid Firoozi, 34; Amin Shokohi, 25; Sadegh Ahmadzadegan, aka Nitr0jen26, 23; Omid Ghaffarinia, aka PLuS, 25; Sina Keissar, 25; and Nader Saedi, aka Turk Server, 26, launched DDoS attacks against 46 victims, primarily in the U.S financial sector, between late 2011 and mid-2013. The attacks disabled victim bank websites, prevented customers from accessing their accounts online and collectively cost the victims tens of millions of dollars in remediation costs as they worked to neutralize and mitigate the attacks on their servers. In addition, Firoozi is charged with obtaining unauthorized access into the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam, located in Rye, New York, in August and September of 2013.

I agree with Jack Goldsmith about this: It's pretty comical that the country that disrupted major installments in Iran is now indicting

Iranians for DDOS attacks on instruments of power that the US used to attack Iran, the nation's banks. It invites a similarly theatrical indictment of Keith Alexander.

> The U.S. indictment is not premised on an international law violation. It is based on violation of U.S. law for harm the Iranians caused inside the United States. The Iranians could invoke precisely the same principle: An Iran indictment for the U.S. cyberattacks would be based on a violation of Iranian domestic law for harm caused in Iran by U.S. officers. In short, the cyberattacks from each nation violated the criminal laws of the other nation.
>
> The United States is likely less concerned with charges of hypocrisy than with deterring attacks on its financial infrastructure. Attorney General Lynch said yesterday that the indictment sends "a powerful message: that we will not allow any individual, group, or nation to sabotage American financial institutions or undermine the integrity of fair competition in the operation of the free market." FBI Director James B. Comey added: "By calling out the individuals and nations who use cyber-attacks to threaten American enterprise, as we have done in this indictment, we will change behavior."
>
> But will the indictments change behavior? The Iranians will almost certainly never appear in the United States and thus never go to trial. John Carlin, the Justice Department's top national security lawyer, argued late last year that indictments for cybercrimes can contribute to deterrence even if the defendants are never prosecuted because they expose the responsible actors and demonstrate more broadly that the United States has

> powerful tools to discover and identify those behind cyberattacks. “The world is small, and our memories are long,” Director Comey said yesterday, explaining the government’s deterrence logic. “People often like to travel for vacation or education, and we want them looking over their shoulder.”
>
> It is hard to assess whether the deterrence effect of the indictments will be large enough to stop further attacks on financial infrastructure or so small that they invite more attacks. Moreover, any deterrence achieved by the indictments comes at the cost of exposing U.S. intelligence capabilities and inviting similarly theatric retaliatory indictments.

The timing of this particular theatrical indictment is all the more interesting given that – as Josh Gerstein points out – the actual indictment was handed up in January, just after the nuclear deal and prisoner swap with Iran was finalized.

> The indictment, handed up by a grand jury in Manhattan on Jan. 21 and unsealed Thursday, charges seven Iranian nationals with launching a cyber assault that impaired the computer systems of major U.S. financial institutions in 2012. One of the defendants is also charged with attempting to take over the controls of a dam in Rye, N.Y.
>
> On the weekend of Jan. 16, the U.S. and Iran implemented the intensely negotiated nuclear deal and carried out a prisoner swap. Under the pact, at least four Americans were released from Iranian prisons, including Washington Post reporter Jason Rezaian. President Barack Obama signed pardons or commutations for seven Iranian nationals who were the subject of U.S. criminal

> cases alleging export violations. Cases were dropped against 14 other Iranians U.S. officials said were unlikely ever to be brought to justice in American courts.

All the more so given this news: last week (apparently after Thursday), Admiral Mike Rogers had a "secret" meeting with Israel's Intelligence Corps Unit 8200, the unit CyberCom partnered with on the StuxNet attack.

> The senior Israeli official noted that one of the subjects that Rogers discussed in Israel was cooperation in the field of cyber defense, particularly in the face of attacks from Iran and Hezbollah. A few days before Rogers' arrival in Israel, the U.S. Justice Department filed indictments for the first time against a group of Iranian hackers on charges of carrying out cyber attacks on banks and essential infrastructure in the U.S. three years ago at the behest of the Iranian Revolutionary Guards. Israel has also faced cyber attacks from Iran and Hezbollah, which according to senior IDF officers were prominent during the fighting with Hamas and its allies in Gaza in the summer of 2014, but have risen in intensity in recent months.

It seems, then, unsealing the indictment is not so much about deterrence, as it is a show (though I'm unclear on the audience — the international public? or the Israelis themselves?) as Israel and the US prepare to ratchet up the cyberwar against Iran.

Reminder: We shut down some functionality in an attempt to isolate the issues that crashed the site last Thursday. We're getting closer but still have comments shut down. Bear with us!