WE HAVE ALWAYS BEEN AT WAR IN IRAN

The NYT has a weird story on new allegations made by Iran, listing a bunch of ways the west has sabotaged it.

> Iran said Tuesday that it had amassed new evidence of attempts by saboteurs to attack Iranian nuclear, defense, industrial and telecommunications installations, including the use of computer virus-infected American, French and German equipment.
>
> [snip]
>
> The accounts of sabotage came three days after the top Iranian lawmaker for national security and foreign policy, Aladdin Boroujerdi, said Iranian security experts haddiscovered explosives planted inside equipment bought from Siemens, the German technology company. Mr. Boroujerdi was quoted in Iran's state-run news media as saying the explosives, which were defused, had been intended to detonate after installation and derail Iran's enrichment of uranium.

It portrays—presumably intentionally—Iran as a crazed country lashing out in all directions.

My favorite line from the story, though, is this one.

> Siemens said its nuclear division had done no business with Iran since the 1979 Islamic Revolution, suggesting that the Iranians, who are prohibited from buying nuclear equipment under United Nations sanctions, bought the booby-trapped equipment from third parties.

The NYT seems to pretend that Iran doesn't know

the US has imposed sanctions on it. It's so funny because I've actually seen NatSec types respond to this article asking whether this admission—effectively Iran listing what it has gotten via illicit channels—isn't more damning to Iran than vice versa. As if Iran and the rest of the world don't know it shops at different markets than the US.

Compare that article with this Ellen Nakashima article repeating Joe Lieberman's claims that Iran is behind some crude cyberattacks on American banks.

> In particular, assaults this week on the Web sites of JPMorgan Chase and Bank of America probably were carried out by Iran, Sen. Joseph I. Lieberman (I-Conn.), chairman of the Homeland Security and Governmental Affairs Committee, said Friday.
>
> "I don't believe these were just hackers who were skilled enough to cause disruption of the Web sites," said Lieberman in an interview taped for C-SPAN's "Newsmakers" program. "I think this was done by Iran and the Quds Force, which has its own developing cyberattack capability." The Quds Force is a special unit of Iran's Revolutionary Guard Corps, a branch of the military.
>
> Lieberman said he believed the efforts were in response to "the increasingly strong economic sanctions that the United States and our European allies have put on Iranian financial institutions."

Somehow Nakashima doesn't distance herself enough from the absurd man making the accusations, because she goes on to make this absurd statement.

> **Unlike the cyberattacks attributed to the United States** and Israel that

> disabled Iranian nuclear enrichment equipment, experts said, **the Iranian attacks were intended to disrupt commercial Web sites**. Online operations at Bank of America and Chase both experienced delays this week.
>
> In a previously undisclosed episode, Iranian cyberforces attempted to disrupt the Web sites of oil companies in the Middle East in August by routing their efforts through major U.S. telecommunications companies, including AT&T and Level 3, according to U.S. intelligence and industry officials. They spoke on the condition that their names not be used because they were not authorized to speak to the press.

Granted, the StuxNet-related malware Gauss at least apparently serves to collect information from commercial bank sites, not disrupt the working of the site (though once the US collects the information they do a whole bunch of disruption through sanctions), but it does attack a bunch of commercial banks. And Flame went after suppliers of Iranian suppliers. So the US and Israeli cyberattacks have been targeting unrelated third parties for years. And yet we're supposed to be outraged because Iran effectively engages in a DNS attack (the kind, of course, that mysteriously brought WikiLeaks down in 2010).

Both these articles come in the wake of a Harold Koh speech saying this:

> **Question 3: Do cyber activities ever constitute a use of force?**
>
> **Answer 3: Yes. Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law.** In analyzing whether a cyber operation would constitute a use of force, most commentators focus on

> whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. *Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.* In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes. Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force.
>
> **Question 4: May a State ever respond to a computer network attack by exercising a right of national self-defense?**
>
> **Answer 4: Yes. A State's national right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof.** As the United States affirmed in its 2011 International Strategy for Cyberspace, "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our

> country."

While I'm sure Koh would argue nothing we've done to Iran constitutes a use of force, certainly Iran could make the case that the US and Israel have been engaging in war on Iran since 2006.

And these articles come at a time when—as Bob Baer notes—we're increasingly losing our intelligence assets in the Middle East, including in coutries aligned with Iran.

> The incidents of the past two weeks suggest it may be time to admit that large parts of the Middle East have fallen off the cliff for the U.S., and large parts of it will be beyond the ken of intelligence for the foreseeable future. Something terrible is going on in Syria, but because it's too risky to put American intelligence officers on the ground there, it's unclear just how terrible it is and how it could be ended. There's simply no way for Americans to tell whether the armed rebellion is dominated by militant Islamists or Jeffersonian democrats. Nor can Americans get a picture of how the men leading the fighting forces on which Bashar Assad is most reliant might be turned.
>
> This problem isn't unique to Syria. A number of countries in the Middle East, from Lebanon to Yemen and from Jordan to Egypt, appear poised to fall into the political abyss. Consider Egypt: since the Muslim Brotherhood came to power, my sources tell me the army there is being purged of officers considered pro-American. I've been told that up to 4,000 officers have been let go, although I have no way to confirm that claim.

Things are quickly changing in the Middle East (and no doubt will change even more rapidly once Obama gets through the election). And whereas Iran once had reason to hide the many ways it had been sabotaged by the US, it seems likely that calculus has changed, both because of desperation in face of the sanctions, and because the power relations in the Middle East are rapidly changing.

The US has been waging war against Iran for years. It seems that Iran now has reason to make that clear.