STUXNET: COVERT OP-EXPOSING CODE IN, COVERT OP-EXPOSING CODE OUT

In this interview between David Sanger and Jake Tapper, Sanger makes a striking claim: that he doesn't know who leaked StuxNet.

> I'll tell you a deep secret. Who leaked the fact? Whoever it was who programmed this thing and made a mistake in it in 2010 so that the bug made it out of the Natanz nuclear plant, got replicated around the world so the entire world could go see this code and figure out that there was some kind of cyberattack underway. I have no idea who that person was. It wasn't a person, it wasn't a person, it was a technological error.

At one level, Sanger is just making the point I made here: the age of cyberwar may erode even very disciplined Administration attempts to cloak their covert operations in secrecy. Once StuxNet got out, it didn't take Administration (or Israeli) sources leaking to expose the program.

But I'm amused that Sanger claims he doesn't know who leaked the information because he doesn't know who committed the "technological error" that allowed the code to escape Natanz. I find it particularly amusing given that Dianne Feinstein recently suggested Sanger misled her about what he would publish (while not denying she might call for jailing journalists who report such secrets).

> What you have are very sophisticated journalists. David Sanger is one of the best. I spoke—he came into my office, he saw me, we've worked together at the Aspen Strategy Institute. He assured me

> that what he was publishing he had worked out with various agencies and he didn't believe that anything was revealed that wasn't known already. Well, I read the NY Times article and my heart dropped because he wove a tapestry which has an impact that's beyond any single one thing. And he's very good at what he does and he spent a year figuring it all out.

Sanger claims, now that DiFi attacked him, he doesn't know who made this "technological error."

But that's not what he said in his article, as I noted here. His article clearly reported two sources—one of them a quote from Joe Biden—blaming the Israelis.

> An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.
>
> "We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know if we were part of that activity."
>
> Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. "It's got to be the Israelis," he said. "They went too far."

And even though Sanger calls this code an

“error,” the quotations he includes show that the President’s briefer and Joe Biden believe it was not an error at all.

In this post, I suggested that the Israelis coded StuxNet to escape, without telling the Americans, so as to undermine American attempts to occupy them with cyberwar to prevent hot war. That is, the implication of Sanger’s article (which he now seems to be trying to retract) is that the Israelis deliberately exposed our cyberwar attack so as to make it more likely they could start a war with Iran.

But there is a far more ominous possibility. The Russians, based on analysis they did at Iran’s Bushehr nuclear plant, have claimed StuxNet might have—and still might—cause Bushehr to explode, effectively setting off a nuclear bomb using code.

Is DiFi so angry at Sanger because he ham-handedly revealed that the Israelis deliberately turned StuxNet into a potential WMD?