STUXNET: A WAY TO NUKE IRAN WITHOUT USING A BOMB?

Last week, Russian Ambassador to NATO, Dmitry Rogozin, told the organization that the computer worm Israel and the US devised to ruin Iran's nuclear program could have led to a catastrophe with the Bushehr nuclear plant like Chernobyl.

> Russia said on Wednesday that NATO should investigate last year's computer virus attack on a Russian-built nuclear reactor in Iran, saying the incident could have triggered a nuclear disaster on the scale of Chernobyl.
>
> [snip]
>
> "This virus, which is very toxic, very dangerous, could have very serious implications," he said, describing the virus's impact as being like explosive mines.
>
> "These 'mines' could lead to a new Chernobyl," he said, referring to the 1986 nuclear accident at a plant in Ukraine, then part of the Soviet Union. "NATO should get to investigating the matter… This is not a private topic."

At first, it seemed like the risk for such a disaster had passed. But the AP has gotten a foreign intelligence report stating that the risk of such a catastrophe remains.

> … such conclusions were premature and based on the "casual assessment" of Russian and Iran scientists at Bushehr.
>
> With control systems disabled by the virus, the reactor would have the force of a "small nuclear bomb," it says.

Which would be rather “neat,” don’t you think? If the US and Israel were to collaborate to pioneer cyberwarfare to effective set off an explosion equivalent to that of a nuclear bomb, all without having to drop the bomb themselves? (The Bushehr reactor is apparently just 12 KM outside of the city of Bushehr, Iran’s chief seaport.)

Richard Clarke provides an explanation (assuming this was not an intentional potential side effect of the US-Israeli plot) for why Stuxnet may still be a risk, in Iran and elsewhere.

> Second, the cyber agent Stuxnet was captured and successfully interrogated. That was not supposed to happen. The attack program had built in to it all sorts of collateral damage controls, including instructions to kill itself after a date certain in 2009. Those controls, most unusual in the world of hackers but common in certain countries covert action programs, failed apparently because the weapon’s designers took the collateral damage controls less seriously than they did the ingenious attack. For a hacker, attacking is always more interesting than pleasing the lawyers. Thus, after laying low the Iranian nuclear enrichment centrifuges at Natanz, the worm made its way from that plant’s supposedly isolated, internal computer network to freedom in cyberspace. Thousands of other computers in Iran were infected, as were many in countries such as Pakistan, India, Indonesia, and even a few in the United States.
>
> [snip]
>
> The problem lies in the fact that the worm ran freely through cyberspace and lots of people caught a copy. One can be sure that highly skilled hackers in several countries are even now taking it apart, modifying it, and getting it

> ready to destroy some other target. They are benefiting from free access to the most sophisticated computer attack weapon ever created. That would not be such a problem except for the fact that the thousands of computer networks that run our economy are essentially defenseless against sophisticated computer attacks.

That is, the Israeli and American hackers behind this cyberattack were no more competent than (or perhaps, just as incompetent as) the spooks that gave Iran nuclear blueprints 11 years ago.

And meanwhile, DOD won’t tell Congress about its cyberwar operations, presumably up to and including Stuxnet.

I guess maybe they’re just crossing their finger and hoping none of the easily predicted unintended consequences would come to pass?