افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نباشد تن من مبـــــاد　　بدین بوم وبر زنده یک تن مــــباد
همه سر به سر تن به کشتن دهیم　　از آن به که کشور به دشمن دهیم

www.afgazad.com　　afgazad@gmail.com

European Languages	زبان های اروپائی

https://www.yahoo.com/finance/news/us-could-destroyed-irans-entire-212300402.html

The US could have destroyed Iran's entire infrastructure without dropping a single bomb

Paul Szoldra

7/6/2016

The United States had a top-secret operation that gave it the ability to shut down much of Iran's infrastructure ahead of a full-scale war, without a single bomb being dropped.

The incredible insight into a highly-classified cyber operation called Nitro Zeus was first exposed in the film "Zero Days" and later corroborated by The New York Times, which interviewed intelligence and military officials who were involved.

The film, directed by Alex Gibney, premieres on Friday.

"We spent hundreds of millions, maybe billions on it," an anonymous National Security Agency source says in the film. "We were inside, waiting, watching. Ready to disrupt, degrade, and destroy those systems with cyber attacks. In comparison, Stuxnet was a back alley operation. [Nitro Zeus] was the plan for a full scale cyber war with no attribution."

The source, whose face and voice are concealed throughout the film, is later revealed to be an actor reciting lines from testimony offered to Director Alex Gibney by CIA and NSA employees.

The focus of the "Zero Days" film is on Stuxnet — the world's first cyber weapon — that was used against Iran's nuclear facilities. But in researching for the film, Gibney found that malicious software was just one small piece of a much larger puzzle.

Nitro Zeus went much further than Stuxnet (the US codename was Olympic Games), giving the NSA the ability to attack Iran's command-and-control systems, so it would not be able to communicate. It could hack in and disable air defenses, so US or Israeli planes would not be shot down. And systems such as the power grid, communications, and financial systems were all infected or backdoored, in case of war.

"This was an enormous, and enormously complex, program," one participant in the program told The New York Times. "Before it was developed, the US had never assembled a combined cyber and kinetic attack plan on this scale."

Stuxnet successfully destroyed roughly one-fifth of Iran's nuclear centrifuges. Nitro Zeus could have done much, much more.

Ultimately, that plan was shelved after Iran slowed its uranium enrichment activities during nuclear negotiations. The US and Iran reached a deal to dismantle much of its nuclear program in January.

But it's frightening to see just how far the US could have gone in its cyber warfare efforts, which included taking out major infrastructure that would no doubt affect Iranian civilians as well.

"When you shut down a country's power grid," the source says. "It doesn't just pop back up. It's more like humpty dumpty. And if all the king's men can't turn the lights back on or filter the water for weeks, lots of people will die."

And that's why, perhaps, some US officials are afraid of a devastating cyberattack very similar to Nitro Zeus someday happening here at home.

Though many cybersecurity experts say the rhetoric is somewhat overblown when talking about hacking into critical infrastructure, if there is one thing the Stuxnet attack proved, it's that sophisticated cyber attacks on the grid or other systems are certainly possible.

"The science fiction cyber war scenario is here," the source says. "That's Nitro Zeus."