# Documentary Explores The Cyber-War Secrets Of Stuxnet

July 4, 2016 4:40 PM ET
Heard on All Things Considered

Alex Gibney's new documentary, *Zero Days*, looks at the Stuxnet worm — a cyber weapon developed by the U.S. and Israel. Gibney talks to NPR's Ari Shapiro about the film and the future of cyber warfare.

ARI SHAPIRO, HOST:

On today's All Tech Considered, one of the best-known cases of cyber warfare hits the big screen.

(SOUNDBITE OF MUSIC)

SHAPIRO: A few years ago, the U.S. and Israel teamed up to sabotage the Iranian nuclear program. Their weapon was a malicious computer worm called Stuxnet. New York Times journalist David Sanger explains what happened when it was unleashed on Iran's Natanz nuclear facility.

(SOUNDBITE OF DOCUMENTARY, "ZERO DAYS")

DAVID SANGER: The United States knew from its intelligence channels that some Iranian scientists and engineers were being fired because the centrifuges were blowing up. And the Iranians had assumed that this was because they would have been making errors, there were manufacturing mistakes. Clearly this was somebody's fault.

SHAPIRO: This is a scene in the new documentary "Zero Days." I asked filmmaker Alex Gibney if this was the first time to our knowledge that digital code was able to create physical destruction in the real world. His answer was a confident yes.

ALEX GIBNEY: That's what makes Stuxnet so special, and that's - it makes it the Pandora's box moment. The chest gets opened, and all these things are now out in the land. And it's been compared in its own way to the dropping of the bomb at Hiroshima and Nagasaki. It's that kind of change in the landscape of weapons.

SHAPIRO: Not in terms of loss of life, obviously.

GIBNEY: No, no, no, no - but in terms of the landscape of weapons. There's a new kind of weapon abroad. And now it's being seen in the Defense Department as a completely different area. So you have the Army. You have the Navy. You have the Air Force. You have the Marines. Now you have cyber.

SHAPIRO: I want to get into the implications of that new kind of weapon. But first, just to follow the story of Stuxnet, it almost becomes a "Frankenstein" tale...

GIBNEY: Yes.

SHAPIRO: ...Because it gets out of the control of its creators.

GIBNEY: That's right.

SHAPIRO: It goes all over the world, and these two virus researchers basically - I mean, they're sort of - and I say this with affection - tech nerds...

GIBNEY: Yes.

SHAPIRO: ..Stumble into this and realize they're discovering something they're not supposed to know about. So let's listen to this clip of Eric Chien describing what was going through their heads.

(SOUNDBITE OF DOCUMENTARY, "ZERO DAYS")

ERIC CHIEN: We were only half joking when we would look at each other and tell each other things like, I'm not suicidal. If I show up dead on Monday, it wasn't me.

SHAPIRO: What went wrong? How did it get out?

GIBNEY: We are fairly certain that what happened was - there were two partners on this code, the United States and Israel. And it was coming out of the CIA and the Mossad, Israelis' intelligence agency. And we believe that the Mossad was being pressured by Bibi Netanyahu to have even bigger and better explosions and to get in more damage more quickly.

SHAPIRO: Bibi Netanyahu, the Israeli prime minister, of course.

GIBNEY: That's correct. And what happened was the Mossad and Israel's NSA, Unit 8200, jiggered with the code to make it more aggressive, and that caused two things to happen. One, it's spread all over the world because in order to spread into Natanz, the idea was that it would just spread rapaciously, and then various IT firms - they would take their, you know, thumb drives or whatever into the Natanz plant it would get in. But it was also spreading out.

And in this case, there was also a flaw in the code. So before that, Stuxnet would sit on somebody's computer without anybody knowing. Now it started to shut computers down. And so people started to get freaked out. They started to report on it. They were sharing this code that was spreading all over the world, and that's where the virus hunters, the detectives of our thriller, discovered it and started to look at what this mysterious code was and realized they'd never seen anything like it before.

SHAPIRO: Now, Israel and the U.S. have never publically confirmed that they created Stuxnet.

GIBNEY: Correct.

SHAPIRO: Your film leaves little ambiguity on that front. What are the implications of this new kind of cyber weapon existing that can do real, physical, tangible harm in the real world?

GIBNEY: Well, it goes way beyond that. So we get to this kind of science fiction cyber scenario that you saw in a movie like "Die Hard" three, where literally...

SHAPIRO: I confess. I didn't see "Die Hard" three.

GIBNEY: OK.

SHAPIRO: So walk me through it.

GIBNEY: You know, suddenly airplanes become weapons. Suddenly water filtration plants start manufacturing poisoned water. Suddenly grids start going down.

SHAPIRO: And is this potential, or is this real? Does the technology...

GIBNEY: It's real.

SHAPIRO: ...Exist today?

GIBNEY: It does. We saw it recently in December in the Ukraine where a huge portion of the Ukrainian grid went down. It's almost universally believed that it was a piece of malware by Russia that caused it to go down. And the only reason it was able to come back as quickly as it did was that Ukraine's grid is so old-school that they actually have manual override functions that most...

SHAPIRO: Wow.

GIBNEY: ...Systems don't have. And that's the scary part because we're, in the United States, more vulnerable than just about anybody else.

SHAPIRO: Who else has these technological capabilities at this point?

GIBNEY: Well, we know that in the wake of Stuxnet, Iran got them very quickly. And they counterattacked. They shut down American banks. They actually tried to hack into a water filtration plant in upstate New York. We know that China has them. Russia has them. And I'm sure there are a number of other countries that are aggressively trying to proceed, even North Korea.

SHAPIRO: And unlike nuclear weapons, unlike chemical or biological weapons, there is no international standard, not even international conversation about the use of offensive cyber weapons like these.

GIBNEY: That's right. As one person says in the film, the only rules at the moment are get away with whatever you can.

SHAPIRO: Do you see any sign that that will change anytime soon?

GIBNEY: Well, I think only if we raise a ruckus. The fact is that one of the most damaging aspects of this new realm of cyber - offensive cyber weapons - is that it is so secret. And we need to raise a ruckus about it in order to make sure that we are discussing this kind of capability so that we know what our government is doing on our behalf.

SHAPIRO: To bring this story of the Stuxnet worm full circle, the U.S. now has a better relationship with Iran than it did when this happened. What do you think the role of Stuxnet was in U.S.-Iranian relations more broadly?

GIBNEY: It's hard to know. You know, initially when Stuxnet launched inside Iran, Iran then actually dramatically increased - once they discovered it was Stuxnet, they dramatically increased the number of centrifuges. So in the short-term, it had just the opposite impact.

But perhaps long-term, Iran felt that, OK, you know, the U.S. is engaged in a kind of sabotage that we can't counter. But we also know that in the back of the mind of President Obama was a cyber-offensive program that we discovered which had been classified prior to our release of a much bigger program targeting our Iran that basically would have shut down the country. So I think that in the back of President Obama's mind when they constructed the deal with Iran was a great opportunity to counterattack if Iran welched on its agreements.

SHAPIRO: So when President Obama spoke in general terms about carrots and sticks, you've pulled back the curtain on what some of those sticks were that we might not have known about.

GIBNEY: That's correct.

SHAPIRO: Can I end by asking about your career more generally? You have made films about the harshest interrogations that the U.S. did after 9/11, the Church of Scientology, now this kind of top-secret cyber-offensive weapon. Do you just choose the most opaque, impenetrable subject and say that's where I'm going next?

GIBNEY: Maybe I got off on the wrong foot. When I did a film called "Enron: The Smartest Guys In The Room," I broke rule number 1A of the filmmaker's handbook, which is never make a film about accounting.

SHAPIRO: (Laughter).

GIBNEY: And that one, I had to explain, you know, accounting, which was at the heart of the Enron thing. So I got used to getting into this complicated territory and trying to figure out ways of making it understandable.

SHAPIRO: Alex Gibney, thank you very much.

GIBNEY: Thank you, Ari.

SHAPIRO: Alex Gibney's new film is called "Zero Days." It comes out in theaters and On Demand July 8.