WIKIPEDIA

# Operation Olympic Games

**Operation Olympic Games** was a covert and still unacknowledged campaign of sabotage by means of cyber disruption, directed at Iranian nuclear facilities by the United States and likely Israel. As reported, it is one of the first known uses of offensive cyber weapons.[1] Started under the administration of George W. Bush in 2006, Olympic Games was accelerated under President Obama, who heeded Bush's advice to continue cyber attacks on the Iranian nuclear facility at Natanz.[1] Bush believed that the strategy was the only way to prevent an Israeli conventional strike on Iranian nuclear facilities.[1]

## Contents

## History

During Bush's second term, General James Cartwright along with other intelligence officials presented Bush with sophisticated code that would act as an offensive cyber weapon. "The goal was to gain access to the Natanz plant's industrial computer controls ... the computer code would invade the specialized computers that command the centrifuges."[1] Collaboration happened with Israel's SIGINT intelligence service, Unit 8200. Israel's involvement was important to the United States because the former had "deep intelligence about operations at Natanz that would be vital to making the cyber attack a success."[1] Additionally, American officials wanted to "dissuade the Israelis from carrying out their own preemptive strike against Iranian nuclear facilities."[1] To prevent a conventional strike, Israel had to be deeply involved in Operation Olympic Games. The computer virus created by the two countries became known as "the bug," and Stuxnet by the IT community once it became public. The malicious software temporarily halted approximately 1,000 of the 5,000 centrifuges from spinning at Natanz.

A programming error in "the bug" caused it to spread to computers outside of Natanz. When an engineer "left Natanz and connected [his] computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed."[1] The code replicated on the Internet and was subsequently exposed for public dissemination. IT security firms Symantec and Kaspersky Lab have since examined Stuxnet. It is unclear whether the United States or Israel introduced the programming error.

## Significance

According to the *Atlantic Monthly*, Operation Olympic Games is "probably the most significant covert manipulation of the electromagnetic spectrum since World War II, when Polish cryptanalysts[2] broke the Enigma cipher that allowed access to Nazi codes."[3] *The New Yorker* claims Operation Olympic Games is "the first formal offensive act of pure cyber sabotage by the United States against another country, if you do not count electronic penetrations that have preceded conventional military attacks, such as that of Iraq's military computers before the invasion of 2003."[4] Therefore, "American and Israeli official action can stand as justification for others."[4]

*The Washington Post* reported that Flame malware was also part of Olympic Games.[5]

# Leak investigation

In June 2013, it was reported that Cartwright was the target of a year-long investigation by the US Department of Justice into the leak of classified information about the operation to the US media.[6] In March 2015, it was reported that the investigation had stalled amid concerns that necessary evidence for prosecution was too sensitive to reveal in court.[7]

Referring to unnamed sources within the CIA and NSA, the documentary film *Zero Days* claims that the Stuxnet/Olympic Games malware was just a small part of a much larger mission to infiltrate and compromise Iran —"Nitro Zeus" (NZ).

# See also

- Operation Merlin

# References

1. Sanger, David (1 June 2012). "Obama Order Sped Up Wave of Cyberattacks Against Iran" (https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0). *The New York Times*. Retrieved 19 October 2012. President Barack Obama "secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyber weapons"
2. Rejewski, Marian. "How Polish Mathematicians Broke the Enigma Cipher." Annals of the History of Computing 3, no. 3 (July 1981): 213–34. doi:10.1109/MAHC.1981.10033.
3. Ambinder, Marc (5 June 2012). "Did America's Cyber Attack on Iran Make Us More Vulnerable" (https://www.theatlantic.com/national/archive/2012/06/did-americas-cyber-attack-on-iran-make-us-more-vulnerable/258120/). *The Atlantic*. Retrieved 19 October 2012.
4. Coll, Steve (7 June 2012). "The Rewards (and Risks) of Cyber War" (http://www.newyorker.com/online/blogs/comment/2012/06/the-rewards-and-risks-of-cyberwar.html). *The New Yorker*. Retrieved 19 October 2012.
5. Nakashima, Ellen (June 19, 2012). "U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say" (https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html). *The Washington Post*. Retrieved June 20, 2012.
6. http://www.wbur.org/hereandnow/2013/06/28/general-leaks-probe (http://www.wbur.org/hereandnow/2013/06/28/general-leaks-probe). Retrieved Sep 18, 2018. Missing or empty `|title=` (help)
7. Ellen Nakashima and Adam Goldman (March 10, 2015). "Leak investigation stalls amid fears of confirming U.S.-Israel operation" (https://www.washingtonpost.com/world/national-security/leak-investigation-stalls-amid-fears-of-

confirming-joint-us-israel-operation/2015/03/10/2a348b1e-c36c-11e4-9ec2-b418f57a4a99_story.html). *Washington Post*. Associated Press. Retrieved April 21, 2016.

# Further reading

- David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, Crown, June 2012, ISBN 978-0307718020

Retrieved from "https://en.wikipedia.org/w/index.php?title=Operation_Olympic_Games&oldid=860601961"

**This page was last edited on 21 September 2018, at 20:07 (UTC).**