US-Israeli Stuxnet Cyber-attacks against Iran: “Act of War”

NATO research team calls Stuxnet attack on Iran an 'act of force'

By RT
Global Research, June 28, 2013
RT 26 March 2013

Theme: Militarization and WMD, US NATO War Agenda
In-depth Report: IRAN: THE NEXT WAR?

Global Research Editor’s Note

The article below originally posted on Global Research on March 26, 2013 sheds light on what is now “official” following the alleged leak of classified information about a covert cyberattack on Iran’s nuclear facilities.

> Retired Marine Gen. James “Hoss” Cartwright has been told he is a target of the probe, NBC News and The Washington Post reported Thursday. A “target” is someone a prosecutor or grand jury has substantial evidence linking to a crime and who is likely to be charged.
>
> The Justice Department referred questions to the U.S. attorney’s office in Baltimore, where a spokeswoman, Marcia Murphy, declined to comment.

US-Israeli Stuxnet Cyber-attacks against Iran: “Act of War”

NATO research team calls Stuxnet attack on Iran an ‘act of force’

Russia Today, March 26, 2013

A group of 20 law and technology experts has unanimously agreed that the Stuxnet worm used against Iran in 2009-2010 was a cyberattack. The US and Israel have long been accused of collaborating on the virus in a bid to damage Iran’s nuclear program.

While that accusations against Washington and Tel Aviv have never been confirmed by either government, a NATO Commission has now confirmed it as an “*act of force.*”

Last year anonymous government officials came forward to tell The New York Times that researchers at the Idaho National Laboratory, which is overseen by the US Department of Energy, passed technical information to Israel regarding vulnerabilities in cascades and centrifuges at Iran’s Natanz uranium enrichment plant.

That information, it is believed, was used to design the Stuxnet worm that set Iran's nuclear program back an estimated two years.

"*Acts that kill or injure persons or destroy or damage objects are unambiguously uses of force*," according to the Tallinn Manual on the International Law Applicable to Cyber Warfare, which lead author Michael N. Schmitt said was written to outline "*how does existing law apply to cyberspace*."

Schmitt told The Washington Times that "*according to the UN charter, the use of force is prohibited, except in self-defense*." Under the guidelines detailed in the Manual, the concept of self-defense could include "*anticipatory self-defense*," which would allow a nation an act of aggression in the event that it perceives a threat as imminent.

The 20 experts were drawn from around the world and took three years to complete the 300-page manuscript, which they were careful to note was not an official policy decision by NATO.

They disagreed over whether the Stuxnet attack qualified as an "*armed attack*," which would constitute the beginning of wartime aggression that, under the Geneva Convention, could be followed by the use of force.

"*We wrote it as an aid to legal advisers to governments and militaries, almost a textbook*," Schmitt told The New York Times. "*We wanted to create a product that would be useful to states to help them decide what their position is. We were not making recommendations, we did not define best practice, we did not want to get into policy*."

US officials have continued to deny American involvement in the attack, but the timing specified by the anonymous sources coincides with an order from President Bush authorizing an increased information exchange with Israel over Iranian nuclear facilities.

During a 2009 conversation with The New York Times, an American official said any secret action against Iran would classify officially as "*science experiments*."

The original source of this article is RT
Copyright © RT, RT, 2013

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **RT**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the

copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca