

## Iran Vows Retaliation Against Cyber or Other Attacks on Its Legitimate Nuclear Facilities

By Stephen Lendman

Global Research, July 07, 2020

Region: <u>Middle East & North Africa</u>, <u>USA</u> Theme: <u>Intelligence</u>, <u>Militarization and</u>

WMD, US NATO War Agenda
In-depth Report: Nuclear War

Iran's legitimate nuclear facilities have no military component, according to the IAEA nuclear watchdog organization and annual US intelligence community assessments of global threats.

Days earlier, Iranian Foreign Minister Zarif explained that legitimate Iranian nuclear sites are subject to unprecedented scrutiny by the IAEA — devoting "92 percent of (its) inspections" to its facilities.

Nuclear armed and dangerous Israel permits no monitoring of its bomb development and producing sites.

The same goes for the US. Yet both countries, NATO, and their imperial allies are waging forever wars in multiple theaters — posing an unparalleled threat to humanity's survival if things are pushed too far.

Over the past week, Iranian facilities experienced unexplained blasts, including a fire, reportedly caused by an explosion (possibly triggered by a cyberattack), causing extensive damage to its Natanz nuclear site last Thursday.

It's Iran's main uranium processing facility, located 279 km south of Tehran.

On Friday, Iran said it determined the cause of what happened. For security reasons, it'll be announced at a later time, a statement said.

Last week, Iranian civil defense chief Gholamreza Jalali said the following:

"Responding to cyberattacks is part of the country's defense might."

"If it is prove(d) that our country has been targeted by a cyberattack, we will respond."

The Natanz Fuel Enrichment Plant is located on a 100,000 square meter site — much of it built eight meters underground. Around a one-story portion is above ground.

Iran's official Islamic Republic News Agency (IRNA) cited Atomic Energy Organization of Iran (AEOI) spokesman Behrouz Kamalvandi, saying that reconstruction of damage to the Natanz complex will begin straightaway, adding:

It'll be on an enlarged site for advanced hardware to replace extensive damage to measuring equipment and precision instruments.

On Sunday, Iranian MP Abolfazl Amouei said a report of damage to Natanz was sent to the IAEA Board of Governors.

Separately, the IRNA news agency suggested that sabotage by the US or Israel may have caused the incident at Natanz, stopping short of accusing either country for what happened, a report saying:

"So far Iran has tried to prevent intensifying crises and the formation of unpredictable conditions and situations," adding:

"But the crossing of red lines of the Islamic Republic of Iran by hostile countries, especially the Zionist regime and the US, means that strategy...should be revised."

Unnamed Iranian officials blamed sabotage for the Natanz incident, stressing that the nation's enemies carried out similar attacks in the past.

In spring 2010, Iranian intelligence discovered Stuxnet malware contamination.

The computer virus infected its Bushehr nuclear facility. At the time, operations were halted indefinitely.

Israel and the US were blamed. Had the facility gone online infected, Iran's entire electrical power grid could have been shut down.

A more destructive virus called Flame malware was known at the time.

According to Internet security experts, it's 20 times more harmful than Stuxnet.

Perhaps a state-of-the-art US and/or Israeli virus today is even more powerful and hard to detect until damage is done.

Iran's military-industrial and legitimate nuclear sites are likely US/Israeli targets for maximum disruption — part of US-led longstanding war on the Islamic Republic by other means.

Separately, Iran's IRGC said its military capability includes onshore and offshore "missile cities" — including underground bunkers and floating platforms.

According to IRGC Admiral Ali Reza Tangsiri:

"Iran has established underground onshore and offshore missile cities all along the coasts of the Persian Gulf and the Gulf of Oman, which would be a nightmare for Iran's enemies" if they preemptive attack the Islamic Republic, adding:

"The IRGC Navy is present everywhere in the Persian Gulf and the Sea of Oman, in every place that the enemy would not even think about."

Reportedly, Iranian long-range ballistic missiles and state-of-the art military vessels are being readied for deployment.

Iran is the region's leading proponent of peace, stability, and mutual cooperation with other nations.

It' militarily preparedness is all about defending the nation if preemptively attacked.

The US, NATO, Israel, and their imperial allies pose the greatest threat to regional and world peace.

Given the grave threat to its security posed by these nations, it's essential for Iran to be prepared to defend the nation if struck.

US rage to transform the Islamic Republic into a vassal state makes unthinkable war on the country possible.

\*

Note to readers: please click the share buttons below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Award-winning author Stephen Lendman lives in Chicago. He can be reached at <a href="mailto:lendmanstephen@sbcglobal.net">lendmanstephen@sbcglobal.net</a>. He is a Research Associate of the Centre for Research on Globalization (CRG)

His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III."

http://www.claritypress.com/LendmanIII.html

Visit his blog site at <u>sjlendman.blogspot.com</u>.

Featured image is from New Eastern Outlook

The original source of this article is Global Research Copyright © Stephen Lendman, Global Research, 2020

## **Comment on Global Research Articles on our Facebook page**

## **Become a Member of Global Research**

Articles by: Stephen Lendman

## About the author:

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III."

http://www.claritypress.com/LendmanIII.html Visit his blog site at sjlendman.blogspot.com. Listen to cuttingedge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network. It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.

**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: <a href="mailto:publications@globalresearch.ca">publications@globalresearch.ca</a>

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: <a href="mailto:publications@globalresearch.ca">publications@globalresearch.ca</a>