GlobalResearch
Center for Research on Globalization

WAR ON IRAN: US Launches New Computer Virus "Weapon of Mass Destruction"

By Finian Cunningham

Global Research, May 29, 2012
29 May 2012

Region: Middle East & North Africa
Theme: US NATO War Agenda
In-depth Report: IRAN: THE NEXT WAR?

The US-led economic war on Iran has been dangerously ratcheted up with the launching of a powerful new computer virus targeting the Islamic Republic's nuclear research facilities and other vital commercial sectors, including the oil and banking industries.

Previously, the Iranian economy and scientific research centres have been hacked with the computer malware or virus known as Stuxnet. That sabotage of Iranian facilities is widely believed to have been the work of American and Israeli military agencies.

Now an even more destructive virus appears to have been unleashed. The so-called Flame malware is said by internet security experts to be 20 times more disruptive to computer systems than Stuxnet. Compared with Stuxnet, which inflicted serious Iranian technical damage nearly two years ago, the latest malware can be seen as virtual weapon of mass destruction.

Again, American and closely collaborative Israeli military agencies are believed to have launched the latest salvo of cyber missiles.

Iranian and Syrian computer systems are reported to be among the main targets of Flame. Although other countries have this week also reported malfunctions from the Flame virus, including Austria, Hong Kong Hungary and United Arab Emirates, precedent would point to its origin as US intelligence, with the motive of adding yet more economic pain on Iran.

Independent internet security firms say that there is no obvious commercial motive for the malware, for example reports of blackmail attempts, and that the most likely instigator of the virus are "state agencies".

Over the past year, the US has been stepping up bilateral economic sanctions on Iran, aimed at crippling the country's central banking and oil sectors that are the backbone of the national economy.

Next month, the US and the European Union are set to tighten the economic embargo on Iran even further with new sanctions lined up to hit the country's international oil trade – some 80 per cent of Iran's national revenues derive from oil and gas sectors.

Moreover, the US, Britain and France, together with Germany and Israel, have been twisting the pressure on Iran at the resumed P5 + 1 talks this month over its nuclear programme, demanding that the country rescind its legal right to enrich uranium.

Tehran has steadfastly refused to suspend its uranium enrichment facilities, which it says it is legally entitled to as a signatory to the Non-Proliferation Treaty, and which are solely for civilian applications, such as energy production and medical radioisotopes.

The evidence certainly points to "regime change" being the thinly veiled objective of the Western powers and that the nuclear issue is a manufactured controversy with which to browbeat Iran. But the war of words goes way beyond browbeating. The US-led international campaign against Iran is tantamount to an all-out covert war, a war that is criminal in its conduct on several counts.

Military threats, invasion of Iranian territory with unmanned aerial vehicles, or drones, financial and economic sanctions, and now intensified computer virus attacks on Iran's telecommunications. This is all but a war of aggression without troops on the ground.

With mainstream news media becoming ever more servile to Western government foreign policy agenda, it is important to remind ourselves of realistic legal and moral perspective here.

Can you imagine how the US, Britain, France or Israel would react if Iran were to shut down their computer systems because it objected to their unlawfully persistent arsenals of actual weapons of mass destruction? Such an Iranian cyber attack would be met with ferocious retaliation or at best would be considered reprehensible, but such a move by Iran would certainly have a lot more legal and moral right than the Western campaign of belligerence towards Tehran.

The panoply of aggression towards Iran is emanating from Western powers that have murderous blood on their hands from the Balkans, Iraq, Afghanistan, Libya, Syria, Somalia, among other places, and this campaign is based on a repetition of outlandish allegations over "weapons of mass destruction". The latest sabotage of Iranian society through computer malware should be seen, and roundly denounced, as yet another war crime by US allies that is pushing the world ever closer to escalation of war.

Finian Cunningham is Global Research's Middle East and East Africa Correspondent

cunninghamfinian@gmail.com

The original source of this article is Global Research

Articles by: Finian Cunningham

About the author:

Finian Cunningham has written extensively on international affairs, with articles published in several languages. Many of his recent articles appear on the renowned Canadian-based news website Globalresearch.ca. He is a Master's graduate in Agricultural Chemistry and worked as a scientific editor for the Royal Society of Chemistry, Cambridge, England, before pursuing a career in journalism. He specialises in Middle East and East Africa issues and has also given several American radio interviews as well as TV interviews on Press TV and Russia Today. Previously, he was based in Bahrain and witnessed the political upheavals in the Persian Gulf kingdom during 2011 as well as the subsequent Saudi-led brutal crackdown against pro-democracy protests.

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

For media inquiries: publications@globalresearch.ca