www.tripolipost.com Facebook.com/thetripolipost

THE TRIPOLI POST

Saturday, June 2-8, 2012 A Weekly Newspaper Price: One Dinar Issue No 374

A massive, data-slurping cyberweapon is circulating in the Middle East, and computers in Iran appear to have been particularly affected, according to a Russian Internet security firm.

Obama Orders Stuxnet Cyber War Against Iran, Effects All Region

Despite the fact that Stuxnet was spreading to machines in the United States and elsewhere and could have contained other unknown errors that might affect US machines, President Barack Obama ordered U.S. officials who were behind the attack to continue the operation.

The information comes in a new report from The New York Times, which asserts that an error in the code led it to spread to an engineer's computer after it was hooked up to systems controlling the centrifuges at Iran's uranium enrichment plant near Natanz. When the engineer left the Natanz facility, he spread it to other machines, writes Times reporter David Sanger, based on a book he has written that will be released next week.

Sources told Sanger that they believed the Israelis introduced the error in the code.

"We think there was a modification done by the Israelis," an unidentified U.S. source reportedly told the president, "and we don't know if we were part of that activity."

Vice President Joe Biden accused the Israelis of going "too far," a source told Sanger.

According to the Times, Obama wondered to advisers whether the attack should be discontinued after Stuxnet began spreading, believing the operation might have been irrevocably compromised.

"Should we shut this thing down?" Obama reportedly asked at a meeting in the White House Situation Room that included Biden and the director of the Central Intelligence Agency at the time, Leon E. Panetta.

But aides advised him that it should proceed since it was unclear how much the Iranians knew about the code, and the sabotage was still working.

At the time, security researchers were still furiously trying to figure out what Stuxnet

Continued on page 2

The Tripoli Post Online Attacked, Put Out of Sight for Four Hours on Friday

Tripoli-- At about 6:00p.m. Tripoli time, on Friday 1 June, The Tripoli Post technical team discovered that The Tripoli Post Online web site was hacked and was out of operation.

The attacker named “Libyan Cyber Army” and said “hacked by The GreaT TeAm... Your Security Is Down Get More Secure Next Time”.

The team worked swiftly to solve the problem and within four hours the site was operating normally.

The IT team identified the offending IP address that was in Tripoli, Libya and hosted by LTT, it identified the method used to hack the Tripoli Post site and was able to close up its vulnerability so hackers do not stop the voice of freedom again.

This is the first time that The Tripoli Post online has been targeted by attackers since it was first launched its web site in 2001.

The attack is a sign of some groups that may have been annoyed by the credibility and persistence of this first private

Continued on page 2