Cyber War -- a 21st Century Reality

by Kismo *Monday, Jan 17 2011, 10:38pm*
international / peace/war / commentary

> Western powers have been slow to develop skills in the crucial theatre of cyber warfare; nevertheless it seems, they have finally engaged. An unsubstantiated report from the UK Telegraph claims that a joint Israeli-US cyber attack may have compromised critical computer systems at Iran's largest nuclear facility.

Iran's Bushehr Facility

In the unlikely event that the integrity of Iran's computer systems had been compromised, redundancies, 'fall-back systems' should have immediately restored integrity. However, the psychological threat component of an exotic viral attack is not without its effect. Any threat to a nuclear facility would have necessitated costly and time-consuming integrity checks and double checks.

In the recent past the USA was forced to engage in very costly systems checks after claims that crucial systems and subsystems had been compromised by a notorious hacker group – we have knowledge of THIS cyber engagement, which cost the US government millions and allowed external engineers to gain access to otherwise highly secured systems, thank you very much, dumbarses! If systems weren't compromised in the first instance they sure were after 'integrity checks' by 'experts' in the field – LOL!

Nevertheless, the US may have learnt a valuable lesson in cyber psywar tactics, which they may have deployed on Iran. The point being that no one can afford to ignore these threats. However, the possibility that external forces gained access to highly secured closed, internal systems is extremely remote.

Report for the UK Telegraph follows:

> **Stuxnet virus attack: Russia warns of 'Iranian Chernobyl'**
> by Con Coughlin
>
> Russian nuclear officials have warned of another Chernobyl-style nuclear disaster at Iran's controversial Bushehr reactor because of the damage caused by the Stuxnet virus,

according to the latest Western intelligence reports.

Russian nuclear scientists are providing technical assistance to Iran's attempts activate the country's first nuclear power plant at the Gulf port.

But they have raised serious concerns about the extensive damage caused to the plant's computer systems by the mysterious Stuxnet virus, which was discovered last year and is widely believed to have been the result of a sophisticated joint US-Israeli cyber attack.

According to Western intelligence reports, Russian scientists warned the Kremlin that they could be facing "another Chernobyl" if they were forced to comply with Iran's tight deadline to activate the complex this summer.

After decades of delays over the plant, which was first commissioned by the Shah in the 1970s, Iran's leaders are demanding that scientists stick to the schedule set last year. They argue that any delay would be a blow to Iran's international prestige.

Bushehr is due to produce its first electricity for Iran's national grid this summer after Russian technicians started loading the first nuclear rods into the reactor last October.

Ali Akbar Salehi, Iran's foreign minister who also serves as head of the country's Atomic Energy Organisation, rejected suggestions earlier this month that the Bushehr opening schedule should be postponed. "All the rumours related to the Westerners' claims that Stuxnet had caused damage to the nuclear plants are rejected," he said.

However, Russian scientists working at the plant have become so concerned by Iran's apparent disregard for nuclear safety issues that they have lobbied the Kremlin directly to postpone activation until at least the end of the year, so that a proper assessment can be made of the damage caused to its computer operations by Stuxnet.

The Iranian government is bitterly opposed to any further delay, which it would regard as another blow to national pride on a project that is more than a decade behind schedule. While Western intelligence officials believe Iran's nuclear programme is aimed at producing nuclear weapons, Iran insists the project's goals are peaceful.

The Russian scientists' report to the Kremlin, a copy of which has been seen by The Daily Telegraph, concludes that, despite "performing simple, basic tests" on the Bushehr reactor, the Russian team "cannot guarantee safe activation of the reactor".

It also accuses the Iranian management team, which is under intense political pressure to stick to the deadline, of "not exhibiting the professional and moral responsibility" that is normally required. They accuse the Iranians of having "disregard for human life" and warn that Russia could find itself blamed for "another Chernobyl" if it allows Bushehr to go ahead.

Yesterday, the New York Times reported that the Stuxnet virus had been developed as a joint project by US and Israeli intelligence officials at Israel's top-secret Dimona project in the Negev desert.

The virus was developed at Dimona over a period of two years before it was planted into Iran's nuclear programme, an operation now widely regarded as the world's most

successful cyber attack.

Hillary Clinton, the US Secretary of State, recently declared that the Stuxnet virus had set Iran's nuclear programme back by several years.

[The entire engagement reeks of psychological warfare -- attack and counter attack. We shall see, as any severe compromise of a nuclear facility would immediately be detectable by numerous global monitors.]
