June 13 2013 | Last updated 4:00 January 01, 1970

gulfnews.com

Opinion | Columnists

Ten consequences of US covert war against Iran

Targeting Iran's nuclear programme through cyber attacks and assassinations will worsen Iran's siege mentality and drive it towards greater aggression

By Seyed Hossein Mousavian | Special to Gulf News
Published: 20:00 May 11, 2013

GULF NEWS

Washington believed that covert action against Iran's nuclear facilities would be more effective and less risky than an all-out war, which could force Tehran to retaliate across the region and divert its current peaceful nuclear programme toward weaponisation. In fact, Mark Fitzpatrick, former deputy assistant secretary of state for non-proliferation said: "Industrial sabotage is a way to stop the programme, without military action,

without fingerprints on the operation, and really, it is ideal, if it works."

The US has a long history of covert operations in Iran, beginning in 1953 with the CIA orchestrated coup d'état that toppled the popularly elected Iranian prime minister Mohammad Mossadegh and installed a dictator, Reza Shah. The US has reorganised its covert operations after the collapse of the shah in 1979.

In early 2009, the New York Times reported that the Bush administration preferred intrusive covert operations aimed at Iran, having concluded that the sanctions imposed by the United States and its allies were failing to curb the country's nuclear programme.

In January 2011, it was revealed that the Stuxnet cyber-attack, an American-Israeli project to sabotage the Iranian nuclear programme, has been accelerated since President Barack Obama first took office. Referring to comments made by the head of Mossad, then US secretary of state Hillary Clinton confirmed the damages inflicted on Iran's nuclear programme have been achieved through a combination of "sabotage and sanctions".

Meanwhile, several Iranian nuclear scientists were assassinated. The New York Times reported that Mossad orchestrated the killings while Iran claimed the attacks were part of a covert campaign by the US, UK

and Israel to sabotage its nuclear programme. Former Republican presidential candidate Rick Santorum boasted that the murders of Iranian nuclear scientists are “a wonderful thing”. John Sawers, former British nuclear negotiator and now the chief of the UK’s intelligence service MI6, advocated in October 2010 for “intelligence-led approach to stopping Iran’s nuclear proliferation”.

There are at least 10 major repercussions arising from the US, West and Israeli policy of launching covert war and cyber-attacks against Iranian nuclear facilities and scientists.

First, cyber war is a violation of international law. According to the UN Charter, the use of force is allowed only with the approval of the UN Security Council in self-defence and in response to an attack by another country. A Nato-commissioned international group of researchers, concluded that the 2009 Stuxnet attack on Iran’s nuclear facilities constituted “an act of force”, noting that the cyber-attack has been a violation of international law.

Second, the US covert operations are a serious violation of the Algiers Accord. The 1981 Algiers Accords agreed upon between Iran and the US clearly stated that “it is and from now on will be the policy of the US not to intervene, directly or indirectly, politically

or militarily, in Iran's internal affairs".

Third, the cyber war has propelled Tehran to become more determined in its nuclear efforts and has made major advancement. According to reports by the International Atomic Energy Agency (IAEA), prior to covert operations targeting the nuclear programme, Iran had one uranium enrichment site, a pilot plant of 164 centrifuges enriching uranium at a level of 3.5 per cent, first generation of centrifuges and approximately 100 kg stockpile of enriched uranium.

Today, it has two enrichment sites with roughly 12,000 centrifuges, can enrich uranium up to 20 per cent, possesses a new generation of centrifuges and has amassed a stockpile of more than 8,000kg of enriched uranium.

Fourth, the strategy pursued has constituted a declaration of war on Iran, and a first strike. Stuxnet cyber-attack did cause harm to Iran's nuclear programme, therefore it can be considered the first unattributed act of war against Iran, a dangerous prelude toward a broader war.

Fifth, by initiating a covert war, the US and the West sacrifice their long-term interests for short-term gains. Such short-sighted policies thicken the wall of mistrust, further complicating US-Iran rapprochement and confidence-building measures.

Sixth, Iran would consider taking retaliatory measures by launching cyber-counter-attacks against facilities in Israel, the West and specifically the US. An unnamed Iranian intelligence official said, “Iran’s intelligence community is in a very good position to design tit-for-tat operations to retaliate against assassinations carried out by western intelligence services. Iran’s response will be extraterritorial and extra-regional. It follows the strategy that none of those who ordered or carried out [the attacks] should feel secure in any part of the world.”

Seventh, Iran is building a formidable domestic capacity countering and responding to western cyber-warfare. Following the Stuxnet attack, Iran’s Supreme Leader issued a directive to establish Iran’s cyber army that is both offensive and defensive. Today, the Islamic Revolutionary Guards Corps (IRGC) has the fourth biggest cyber army in the world. Israel’s Institute for National Security Studies (INSS) acknowledged that IRGC is one of the most advanced nations in the field of cyberspace warfare.

Eighth, Iran now has concluded that information gathered by IAEA inspectors has been used to create computer viruses, facilitate sabotage against its nuclear programme and the assassinations of nuclear scientists. Iranian nuclear energy chief stated that the UN nuclear watchdog [IAEA] has been infiltrated by

“terrorists and saboteurs.” Such conclusions have not only discredited the UN Nuclear Watchdog but have pushed Iran to limit its technical and legal cooperation with the IAEA to address outstanding concerns and questions.

Ninth, worsening Iranians siege mentality by covert actions and violations of the country’s territorial sovereignty could strengthen the radicals in Tehran to double down on acquiring nuclear weapons. Iran could be pondering now the reality that the US is not waging a covert war on North Korea (because it possesses a nuclear bomb), Muammar Gaddafi lost his grip on power in Libya after ceding his nuclear programme, and Iraq and Afghanistan were invaded (because they had no nuclear weapon).

Tenth, the combination of cyber-attacks, industrial sabotage and assassination of scientists has turned public opinion within Iran against western interference within the country and instead has garnered more support for the Iranian government’s nuclear policy. At the same time, such provocative western measures have convinced the Iranian government that the main issue is not the nuclear programme but rather regime change.

Hossein Mousavian is associate scholar at Princeton

University. He served as the Head of Foreign Relation Committee of Iran's National Security Council from 1997 to 2005. He is author of "The Iranian Nuclear Crisis: A Memoir," published by Carnegie Endowment for International Peace in 2012.