EUI Working Papers

MWP 2012/17
MAX WEBER PROGRAMME

THE COVERT WAR AGAINST IRAN'S NUCLEAR PROGRAM: AN EFFECTIVE COUNTERPROLIFERATION STRATEGY?

Richard Maher

EUROPEAN UNIVERSITY INSTITUTE, FLORENCE
MAX WEBER PROGRAMME

The Covert War against Iran's Nuclear Program: an Effective Counterproliferation Strategy?

RICHARD MAHER

EUI Working Paper **MWP** 2012/17

ISSN 1830-7728

Printed in Italy
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu
cadmus.eui.eu

Abstract
For nearly a decade the United States and some of its key allies have sought to disrupt, delay, and potentially reverse Iran's nuclear program through diplomatic pressure, economic sanctions, and veiled threats of military attack, all with little or no success. As Iran inches closer to acquiring a nuclear weapons capability, the United States and Israel have embarked on a bolder and far riskier strategy of covert action to thwart Iran's nuclear progress, which has included assassinating Iranian nuclear scientists, infiltrating and sabotaging procurements networks on which Iran relies for parts and equipment for its nuclear program, and unleashing cyber attacks against Iran's nuclear infrastructure. Despite the increased prominence of covert counterproliferation efforts against Iran, there has been little effort by scholars and other observers to evaluate their effectiveness. While the goal of covert action has been to provide more time for diplomacy and economic sanctions to work—rather than to permanently cripple Iran's nuclear program—covert action has become increasingly ineffective, self-defeating, and counterproductive. Contrary to its advocates' claims, it will make diplomacy and a future compromise more difficult by reinforcing mutual suspicions, hostility, and antagonisms between Washington and Tehran.

Keywords
Covert action; USA; Iran; Israel; nuclear capability.

Richard Maher
Max Weber Programme, 2011-2012

Introduction

For the past decade, the United States and its allies have pursued a number of strategies to disrupt, delay, and potentially reverse Iran's uranium enrichment program—economic and diplomatic sanctions, censure at the United Nations, and veiled threats of military action—all with little or no success. As Iran's enrichment program continues to make progress, and Tehran inches closer to a nuclear weapons capability, the United States and in particular Israel have accelerated a bolder and far riskier strategy to frustrate Iran's nuclear ambitions; a sustained and multifaceted campaign of covert action, which has included assassinating and intimidating Iranian nuclear scientists, infiltrating and sabotaging black market procurement networks on which Iran relies for crucial parts and equipment for its nuclear program, and unleashing cyber attacks against Iran's nuclear infrastructure.

These actions, if done in a domestic context, would plainly be illegal. If committed against the United States, many of these actions would fit the standard U.S. definition of international terrorism. Many Americans would consider these actions a flagrant breach of international law and, if traced back to a state, tantamount to acts of war. The covert campaign against Iran's nuclear program is thus beginning to blur into actual warfare.

There has been little effort by scholars and other analysts to evaluate and assess whether this covert campaign has been or will be effective in substantially delaying or disrupting Iran's nuclear program at acceptable cost and political risk. This paper argues that rather than proving to be an effective means of slowing Iran's nuclear progress, these covert actions are becoming increasingly ineffective, self-defeating, and counterproductive. While covert action might have achieved a few tactical successes, it is not a viable long-term strategy, either in the context of Iran's enrichment program or as a general approach to counterproliferation. Iran has adapted its behavior to limit its vulnerability to sabotage and other clandestine activity, and the covert war has reinforced the suspicious and mutually hostile relationship between Washington and Tehran, making future diplomacy and a possible compromise more difficult. The covert campaign may also lead to unintended and unpredictable consequences, including an escalation of the nuclear crisis that could lead to an overt military confrontation.

The rest of this paper proceeds as follows. The next section briefly examines the use of covert strategies in response to nuclear proliferation threats. The following three sections analyze in turn the main covert tactics and strategies the United States and/or Israel have used to attempt to disrupt and delay Iran's nuclear program: assassination, sabotage, and cyber attacks. The paper then evaluates the effectiveness of covert counterproliferation strategies, finding them largely ineffective, self-defeating, and counterproductive. The conclusion briefly describes two key implications following from this analysis and considers a policy alternative for dealing with the Iranian nuclear challenge.

A New Era of Covert Counterproliferation?

The United States and its allies have imposed unprecedented diplomatic and economic pressure on Tehran to suspend its uranium enrichment program, to grant international nuclear inspectors complete access to its nuclear facilities and personnel, and to provide a full accounting of its current and past nuclear activities. New sanctions on Iran's banking sector could effectively shut off Iran's Central Bank from global credit markets. The European Union, which accounts for 18 percent of Iranian oil exports, has imposed an embargo on all Iranian oil imports, effective July 1, 2012. Scholars and political commentators in the United States and Israel hotly debate the merits and feasibility of an American or Israeli military attack against Iran's main nuclear facilities. Intense speculation abounds over whether Israel will attack Iran's nuclear facilities sometime in the next twelve months.[1]

The traditional methods the United States has used to prevent countries from developing nuclear weapons have included codifying states' rights and obligations through a dense web of treaties and international agreements, persuading countries that it is not in their interest to have nuclear weapons, implementing export controls to deny countries the requisite technology and equipment to build nuclear weapons, fostering international cooperation to interdict the transport of illicit nuclear

[1] Matthew Kroenig, "Time to Attack Iran," *Foreign Affairs* 91(1) (January-February 2012), pp. 76-86; Ronen Bergman, "Will Israel Attack Iran?" *New York Times Magazine*, January 29, 2012.

material, and, as in the case of Iraq in 2003, overt military intervention.[2] While some combination of all these measures—short of military intervention—have been used against Iran, the United States and some of its main allies have used covert action, a less traditional counterproliferation strategy, in an attempt to exploit Iran's perceived vulnerabilities. Rather than seeking to permanently cripple or disable Iran's enrichment program, the main objective of the covert campaign has been to slow down Iran's nuclear progress so that other strategies, namely sanctions and diplomacy, have more time to work.

While in practice covert action may take many forms, conceptually it is simply any activity for which the United States or another country wishes to conceal its identity and maintain plausible deniability.[3] While covert action has existed since the time of Thucydides, during the Cold War it became a routine instrument of statecraft on both sides of the Iron Curtain. For many Cold War strategists and analysts, there was a strong strategic rationale for covert action during that period. The United States faced an implacable ideological and military adversary across the globe, yet direct military confrontation between two nuclear superpowers would have carried far too much risk. Covert action in the so-called Third World, including paramilitary operations, propaganda campaigns, coups, clandestine support for military juntas, assassination, and secretly influencing elections and other political outcomes, seemed vital to preserve the strategic balance.

Following the Cold War, however, many analysts, intelligence officials, and policy makers began to question whether the United States would or even should continue to rely on covert action in pursuit of its strategic objectives. A number of covert operations during the Cold War became synonymous with political and strategic disaster, such as the Bay of Pigs fiasco in 1961, attempts to destabilize North Vietnam, and the Iran-Contra scandal in the mid-1980s.[4] Other covert actions, such as the CIA-orchestrated coup in Iran in 1953, which deposed the democratically elected Mohammad Mossadegh and reinstated the shah, may have been a short-term tactical success but continues to resonate with Iranians to this day and adds to their sense of grievance against the United States. To many, covert action seemed inconsistent, or at least in tension, with the values and principles of liberal democracy, such as openness and transparency, self-determination, adherence to international law, and respect for state sovereignty.[5]

Traditional security threats such as nuclear proliferation and terrorism took on new dimensions in the post-Cold War period, especially after the September 11 terrorist attacks. Once again covert action seemed like a necessary and compelling strategy to counter these threats. New proliferation challenges such as North Korea and Iran seemed impervious to diplomacy and negotiation. As John Sawers, chief of Britain's MI6, said in a 2010 speech, diplomacy alone is unlikely to stop nuclear proliferation. "We need intelligence-led operations to make it more difficult for countries like Iran to develop nuclear weapons," he said. "The longer international efforts delay Iran's acquisition of nuclear weapons technology, the more time we create for a political solution to be found."[6]

---

[2] See Jason D. Ellis and Geoffrey D. Kiefer, *Combating Proliferation: Strategic Intelligence and Security Policy* (Baltimore: Johns Hopkins University Press, 2004); Lee Feinstein and Anne-Marie Slaughter, "A Duty to Prevent," *Foreign Affairs* 83(1) (January-February 2004), pp. 136-150; Ashton Carter, "How to Counter WMD," *Foreign Affairs* 83(5) (September-October 2004), pp. 72-85.

[3] Bruce D. Berkowitz and Allan E. Goodman, "The Logic of Covert Action," *The National Interest*, No. 51 (Spring 1998), pp. 38-46.

[4] See Jim Rasenberger, *Brilliant Disaster: JFK, Castro, and America's Doomed Invasion of Cuba's Bay of Pigs* (New York: Scribner, 2011); Richard H. Schultz, *The Secret War against Hanoi: The Untold Story of Spies, Saboteurs, and Covert Warriors in North Vietnam* (New York: Harper Collins, 1999); Lawrence E. Walsh, *Firewall: The Iran-Contra Conspiracy and Cover-Up* (New York: W. W. Norton, 1997).

[5] For discussions of the tension between liberal democracy and covert action, see Charles R. Beitz, "Covert Intervention as a Moral Problem," *Ethics & International Affairs* 3(1) (March 1989), pp. 45-60; David P. Forsythe, "Democracy, War, and Covert Action," *Journal of Peace Research* 29(4) (November 1992), pp. 385-395; Allan E. Goodman, ed., *The Need to Know* (New York: Twentieth Century Fund Press, 1992); Gregory F. Treverton, "Imposing a Standard: Covert Action and American Democracy," *Ethics & International Affairs* 3(1) (March 1989), pp. 27-43.

[6] Quoted in William Maclean, "Not-So-Covert Iran War Busy Times, Raises Tensions," *Reuters*, January 18, 2012. Similarly, former Vice President Dick Cheney said that America would have to embrace "the dark side" in its post-September 11 counterterrorism and counterproliferation efforts.

The United States and Israel have been waging a covert campaign against Iran's nuclear program for over a decade.[7] Meir Dagan, who headed Mossad, Israel's secret intelligence agency, from 2002 to 2011, concentrated his efforts to thwart Iran's nuclear progress largely on covert actions. George W. Bush authorized an increase in covert actions against Iran months before leaving office, and the Obama administration has accelerated many of these programs. Since the end of the Clinton presidency, the United States has spent hundreds of millions of dollars on various efforts to sabotage Iran's nuclear program. Though it has been one of the United States' most closely guarded state secrets, the covert campaign against Iran has become increasingly active and visible in recent years.[8]

To its advocates, covert action has slowed Iran's enrichment program in a way political pressure, diplomatic isolation, economic sanctions, and the threat of military attack have been unable to accomplish. Proponents argue that covert action is an expedient middle ground between an overt military attack, which would likely have dangerous and unpredictable consequences, and continuing to wait for economic and political pressure to change Iran's behavior. Covert action puts fewer Americans in harm's way and, without deploying large conventional ground forces, provides a comparatively low-cost means to fight proliferation challenges. Covert war is also less provocative than an overt military attack, arguably allowing Iran an opportunity to back down without losing face.

Another potential benefit of covert action, according to its proponents, is that it creates uncertainty about who is responsible for an attack. This can be strategically beneficial since it is more difficult for a country to retaliate if it is not fully certain of the origins of an attack or the identity of the attacker. When it is clear who is behind an attack, domestic political forces demanding revenge and retaliation are often overwhelming. So while Iran may have its suspicions about who is behind these covert attacks, it has been unable thus far to provide any credible evidence linking either the United States or Israel to any of the instances in which sabotage has been suspected.

To its critics, however, covert action is often reckless, unlawful, ineffective, and counterproductive. It is a sign of desperation; states rely on covert action only when there are no viable policy alternatives. Covert action operates in opaque realms beyond public scrutiny. By its very nature, there is less public debate over the potential benefits versus the risks and costs, and covert operations are often used to hide political aims governments wish to keep from public scrutiny. Covert actions do not have the same level of legal restrictions, accountability mechanisms, and Congressional oversight that other government initiatives face. Policymakers often seem to overemphasize the potential benefits of covert action while discounting or minimizing the potential risks and costs. Covert actions often transgress ethical principles regarding laws of war and self-defense, and the consequences are often damaging and bring unintended consequences. There is a propensity for covert actions to backfire, damaging U.S. credibility and tarnishing its image.

While covert action may thus seem expedient, especially when more conventional strategies prove ineffective or unviable, covert action often cannot be kept secret forever, has consequences and repercussions often far different than what was expected or anticipated, and undermines the U.S. commitment to democracy, an open society, the rule of law, and the self-determination of peoples. In sum, it is almost always a bad idea.[9]

This paper now presents in turn the three main covert strategies the United States and/or Israel have used to disrupt and delay Iran's nuclear program, analyzing their individual and collective ability to substantially delay Iran's nuclear progress.

Assassinating Iranian Nuclear Scientists

By far the most controversial element of the covert campaign against Iran have been the assassinations of Iranian scientists connected to the nuclear program. At least five Iranian nuclear scientists have

[7] See Catherine Collins and Douglas Frantz, *Fallout: The True Story of the CIA's Secret War on Nuclear Trafficking* (New York: Free Press, 2011).

[8] Scott Shane, "Adversaries of Iran Said to Be Stepping Up Covert Actions," *New York Times*, January 11, 2012.

[9] Gregory F. Treverton, *Covert Action: The Limits of Intervention in the Postwar Order* (New York: Basic Books, 1987).

been killed since 2007, with at least four of these coming in the past two years alone.[10] The United States has condemned the killings and categorically denied any involvement. Senior administration and intelligence officials are reported to be outraged over the escalating number of killings, fearing that Iranian retaliation may put American lives at risk. The Israeli response to the killings has been more vague, with the Israeli government neither confirming nor denying Israeli involvement.[11]

The most recent assassination took place in January 2012 when Mostafa Ahmadi Roshan, a 32-year-old professor at a technical university in Tehran and a department supervisor at the Natanz uranium enrichment plant, was killed during his morning commute to work. On a busy street in downtown Tehran, an unidentified assassin on a motorcycle attached a limpet mine (also known as a magnet bomb) to Roshan's car window, killing him instantly.[12] Ardeshir Husseinpour, a 44-year-old nuclear physicist at the Isfahan uranium conversion plant, died in January 2007 under mysterious circumstances, allegedly related to "gas poisoning," according to Iranian officials. Massoud Ali Mohammadi, an expert in quantum physics at Tehran University, died when a booby-trapped motorcycle exploded outside his house.[13] On November 29, 2010, Majid Shahriari, an expert on nuclear chain reactions, was killed, like Roshan, during his morning commute. On the same morning, Fereydoon Abbasi narrowly escaped a similar attack. Following the failed assassination attempt, Abbasi, a longtime member of the Islamic Revolutionary Guards, was appointed head of the Iranian Atomic Energy Organization (IAEO). On July 23, 2011, two gunmen shot and killed Darioush Rezae Nejad, a nuclear physicist and researcher for the IAEO.[14]

Assassination has been against U.S. law for more than three decades. The Church Committee published a series of reports in the mid-1970s detailing CIA plots in the 1950s and 1960s to kill foreign leaders, including Fidel Castro (who survived no less than eight assassination plots), Patrice Lumuma of the Congo, Ngo Dinh Diem of South Vietnam, and Rafael Trujillo of the Dominican Republic. The Church report stated that assassination, with rare exceptions, "violates moral precepts fundamental to our way of life." Gerald Ford signed an executive order in 1976 banning assassination, and Ronald Reagan reiterated the ban with Executive Order 12333, which stated that "No person employed or acting on behalf of the United States Government shall engage in, or conspire to engage in, assassination." Providing information or intelligence to assist another country to carry out an assassination would violate the ban. Executive Order 12333 is still in effect, and every U.S. president since Ford has upheld the prohibition on assassination.[15]

Israel has used assassination as a tool of statecraft more than any other country, employing it against various perceived enemies since the country's founding in 1948 and developing considerable skill and expertise in its use. Israel's first targeted killing occurred in 1956, when Mossad agents killed

---

[10] For a timeline of the killings, see Tom Burgis, "Timeline: Assassinated Iranian Scientists," *Financial Times*, January 11, 2012, http://blogs.ft.com/the-world/2012/01/timeline-assassinated-iranian-scientists/#axzz1lcOz0T6i

[11] Mysterious killings and disappearances of Iranians with connections to the country's nuclear or military programs predate the recent spate of killings of nuclear scientists. In July 2001, for example, Ali Mahmoudi Mimand, at the time called the father of Iran's missile program, was found dead in his office with a gunshot wound to the head. The killer has never been caught, though Israel is suspected to be behind the murder.

[12] Among the several jobs Roshan appears to have had was procurement officer at Natanz, which may explain why he was a target. In this capacity, Roshan would have been involved in Iran's efforts to acquire equipment, parts, and technology through international black markets for Iran's enrichment program. See Alan Cowell and Rick Gladstone, "Iran Reports Killing of Nuclear Scientist in 'Terrorist' Blast," *New York Times*, Jan 11, 2012.

[13] Mohammadi's killing was seen in Tehran's political and scientific circles as a possible act of revenge perpetrated by the clerical regime. Mohammadi was a known sympathizer of the opposition Green movement and of the anti-government protestors following the fraudulent 2009 presidential election in Iran.

[14] Bergman, "Will Israel Attack Iran?"

[15] U.S. presidents have slowly moved away from the categorical ban on assassination embodied in Executive Order 12333, however. Since the September 11 attacks, the United States has adopted a policy of targeted assassination of Taliban and al Qaeda militants. See Ward Thomas, "The New Age of Assassination," *SAIS Review* 25(1) (Winter/Spring 2005), pp. 27-39. Both Bush and Obama administration officials, as well as legal scholars, have drawn a distinction between assassination, which would violate U.S. law, and targeted killing, for which the president has Congressional authorization. For a legal rationale that targeted killings do not violate U.S. law, see John Yoo, *War by Other Means: An Insider's Account of the War on Terror* (New York: Atlantic Monthly Press, 2006), chapter 3.

Mustafa Hafez, the head of the Egyptian secret service. Since then Israel has targeted for assassination dozens of Palestinian militants, persons accused of being Holocaust collaborators, and foreign scientists and military officials involved in weapons of mass destruction (WMD) programs targeted against Israel. Mossad conducted a two-decade long campaign to kill the Black September members involved in the 1972 Munich Olympics massacre, and targeted for assassination Iraqi scientists working on Iraq's nuclear weapons program in the late 1970s and early 1980s.[16]

Despite Israel's considerable operational and logistical skill in these types of operations, it would be virtually impossible for Mossad's sabotage-and-assassination unit, known as Caesarea, to operate inside Iran. As a result, Israel likely has received help from groups inside Iran, possibly the People's Mojahedin of Iran (MEK) and/or Jundallah, exiled Iranian groups that advocate the overthrow of Iran's clerical regime. The U.S. State Department lists both groups as terrorist organizations.

In addition to eliminating valuable human assets from Iran's nuclear program, supporters of the covert assassination campaign claim it produces what Mossad calls "white defection." That is, fewer Iranian scientists volunteer to work on the nuclear program, and those already working on the program become so concerned for their safety that they request to be transferred to civil projects, depriving Iran's nuclear program of even more technical and scientific expertise.[17]

Is the covert assassination campaign worth the effort, resources, and risk, however? In the absence of a formal state of war, nuclear scientists are not thought to be legitimate targets of assassination.[18] Apart from the question of whether such killings are morally justifiable, a covert assassination campaign can lead to unintended consequences for the attacker.[19] There is a danger these killings could further erode the international norm against assassination, which could put high-ranking American officials at risk.[20] Iran may ultimately seek revenge, and the resulting bloodshed could be vastly disproportionate to the value of eliminating a few Iranian scientists. Iran could use proxy groups such as Hezbollah or Hamas or its own Revolutionary Guard forces to assassinate targets outside its borders. In the 1980s and 1990s Iran killed several exiled Iranian political dissidents in Europe and other countries in southwest Asia, which was partly why Iran was originally placed on the State Department's list of state sponsors of terrorism.

Israel experienced such repercussions following the assassination of the Hezbollah leader Sheik Abbas Musawi in 1992. A month after Musawi's killing, Hezbollah operatives blew up the Israeli Embassy in Buenos Aires, killing 29 people and injuring more than 200. Two years later, in July 1994, a suicide bomber struck a Jewish community center, also in Buenos Aires, killing 85.[21] While the killing of Musawi may have been a tactical success for the Israelis, it turned out to be a

---

[16] On Israel's history of using assassination against its enemies, see Simon Reeve, *One Day in September: The Full Story of the 1972 Munich Olympic Massacre and the Israeli Revenge Operation "Wrath of God"* (London: Faber & Faber, 2001); Michael L. Gross, "Fighting by Other Means in the Mideast: A Critical Analysis of Israel's Assassination Policy," *Political Studies* 51(2) (June 2003), pp. 350-368; Ami Pedahzur, *The Israeli Secret Services and the Struggle Against Terrorism* (New York: Columbia University Press, 2009), especially chapter 1.

[17] Bergman, "Will Israel Attack Iran?"

[18] William Tobey, "Nuclear Scientists as Assassination Targets," *Bulletin of the Atomic Scientists* 68(1) (January/February 2012), pp. 61-69. See also Michael Walzer, *Just and Unjust Wars: A Moral Argument With Historical Illustrations, 4e* (New York: Basic Books, 2006), p. 219.

[19] Bungled assassination attempts like that of the Hamas leader Khaled Meshaal in Jordan also provide a cautionary lesson about the risks and dangers of targeted killings.

[20] On the weakening of the norm against assassination, see Ward Thomas, "Norms and Security: The Case of International Assassination," *International Security* 25(1) (Summer 2000), pp. 105-133. See also Ward Thomas, *The Ethics of Destruction: Norms and Force in International Relations* (Ithaca, N.Y.: Cornell University Press, 2001), chapter 3; Michael L. Gross, *Moral Dilemmas of Modern War: Torture, Assassination, and Blackmail in an Age of Asymmetric Conflict* (New York: Cambridge University Press, 2010), chapter 5.

[21] Ronen Bergman, "Bracing for Revenge," *New York Times*, February 18, 2008.

strategic disaster.[22] The assassinations may even have allowed Iran to garner international sympathy, giving the clerical regime a rare propaganda victory.

Irrespective of the threat of Iranian retaliation, Iran's nuclear program is now too advanced for the killing of a few of its scientists to cause a prolonged, let alone decisive, setback. The program involves hundreds of scientists, engineers, and technicians throughout the country, and it is highly unlikely that anyone is truly irreplaceable. As William Tobey, who served on the National Security Council under three administrations, says, "It is difficult to imagine a country having a scientific infrastructure large enough to support a nuclear weapons program, but too small to sustain a viable effort after the loss of even several individuals."[23] Moreover, Iran's nuclear program is shrouded in secrecy, making it difficult for a foreign intelligence agency to know who is important, much less vital, to the program's success.

Partly in response to the killings, Iran has placed even greater restrictions on international nuclear inspectors' access to its nuclear scientists. For years Iran has accused the International Atomic Energy Agency (IAEA) of leaking information about its nuclear program to the United States and other Western governments. While Iran may have genuine concern for the safety of its scientists, it could also be using the assassinations as a pretext to limit even further its cooperation with international nuclear inspectors. Iran claims that if the names of its nuclear scientists became public they would immediately become vulnerable to attack by foreign governments.[24]

Iran now takes measures to better protect its most important nuclear scientists.[25] Mohsen Fakrizadeh, widely believed to be the scientific head of Iran's nuclear program, now has an extensive security detail, and his lectures at Tehran University were suspended as a precautionary measure. Abbasi is likewise heavily protected wherever he travels. In sum, the covert assassination campaign is unlikely to cause a prolonged disruption to Iran's nuclear program, hardens Iran's sense of siege and persecution, and will cause Iran to become even more defiant and uncooperative.

Sabotaging the Iranian Nuclear Program's Procurement Networks

A second strategy the United States and its allies have used to try to disrupt and delay Iran's nuclear progress is infiltrating and sabotaging the supply networks on which Iran relies for much of the equipment and technology for its nuclear program. Because of international sanctions, international export controls limiting the transfer of technology that could be used to develop nuclear weapons, and Iran's own poor industrial base, Iran is heavily dependent on foreign suppliers, shady middlemen, and various black market traffickers to acquire the specialized equipment such as vacuum pumps and valves it needs for its centrifuges and its uranium enrichment program more broadly. American intelligence agencies have supplied Iran with faulty parts, blueprints, and software for years, and as Iran is forced to cast a wider net for the parts and equipment it needs, there are more opportunities for the United States and Israel to sabotage the supply chain.[26]

As a result, nothing Iran acquires on the black market is perfectly safe from tampering, and Iran's nuclear program has experienced a number of accidents and mishaps over the past decade that could be the result of sabotage. An April 2006 explosion at Natanz, allegedly due to manipulated parts Iran had imported from Turkey, destroyed 50 centrifuges. In January 2007, centrifuge parts Iran had purchased from a middleman in Eastern Europe were found to be defective.[27] Tampering and sabotage can be especially effective against specialized equipment such as centrifuges, highly sophisticated and temperamental machines that will not work properly if there is only a slight defect. And because

---

[22] Hezbollah has also vowed to take revenge for the suspected Israeli killing of Imad Mughniyah, one of its top leaders, in Damascus in 2008. Mughniyah was allegedly responsible for Hezbollah military operations in southern Lebanon since the early 1990s.

[23] Tobey, "Nuclear Scientists as Assassination Targets."

[24] Abbasi, for example, was on the UNSC sanctions list because of his ties to Iran's nuclear program.

[25] Rick Gladstone, "Iran Tightens Its Security for Scientists After Killing," *New York Times*, Jan 17, 2012.

[26] Collins and Frantz, *Fallout*.

[27] Ronen Bergman, *The Secret War with Iran: The 30-Year Clandestine Struggle Against the World's Most Dangerous Terrorist Power* (New York: Free Press, 2008).

centrifuges operate in long cascades, a slight defect in one could potentially cause massive disruptions, producing a domino effect that could lead to major damage.

Efforts to sabotage the supply chain and procurement network on which Iran relies have taken many forms. The CIA may persuade a shady middleman to sell defective parts to Iranian buyers. In 2000, for example, the CIA used a former Russian scientist to provide Iran with erroneous blueprints for a nuclear weapon.[28] The triggering device in the blueprints had a hidden design flaw, making it inoperable. The operation appears to have backfired, however. The Russian tipped off the Iranians to the flawed part in the blueprints (and the parts that were accurate), so instead of setting Iran's nuclear efforts back the CIA may have inadvertently given the Iranians valuable and accurate information on how to create a nuclear weapon.

The CIA can also provide defective or manipulated equipment to front companies, which then sell the tampered parts to Iran. Front companies often start by delivering legitimate, working equipment to Iran, gaining the regime's trust. Once trust has been established, the front company then begins to deliver defective items intended to sabotage Iran's nuclear activities. Alternatively, equipment can be bugged to relay crucial intelligence on how and where the equipment is being used. David Albright, president of the Institute for Science and International Security (ISIS) and a former UN weapons inspector, has told, for example, how vacuum pumps Iran acquired on the black market, while produced in Germany, had also been worked on by the Oak Ridge and Los Alamos national laboratories in the United States. As Albright said, the U.S. labs modified the pumps "to bug them or to make them break down under operational conditions. If you can break the vacuum in a centrifuge cascade, you can destroy hundreds of centrifuges or thousands if you are lucky."[29]

In one of the most high-profile attempts at sabotaging Iran's nuclear program, the CIA used the Tinners, a Swiss family of engineers who played a key role in the Abdul Qadeer Khan nuclear proliferation network, as moles for the agency. The Tinners tipped off the CIA to a delivery of centrifuge parts to Libya, which ultimately led to the discovery and dismantlement of Libya's nascent nuclear weapons program and to Khan's nuclear smuggling network. Over a period of four years, CIA agents paid the Tinners as much as $10 million.[30]

In addition to sabotaging Iran's procurement networks, the United States and Israel are also suspected of playing a role in a series of mysterious explosions in Iran over the past several years, with at least two dozen unexplained blasts around Iran in the past two years alone. Oil facilities, gas pipelines, trains, and military bases have been targeted, damaged, or destroyed. The scale, scope, and success of these operations suggest there has been some inside support involved.

The biggest and one of the most mysterious explosions took place on November 12, 2011, at a Revolutionary Guards military base 30 miles west of Tehran and three miles west of the town of Bidganeh that was used as a testing site for advanced solid-fuel missiles. The blast killed 17 people, including Gen. Hassan Tehrani Moghaddam, the head of Iran's missile program, and a close personal associate of Iran's supreme leader, Ayatollah Ali Khamenei. The blast was a major setback for Iran. Not only did it kill a number of experts and specialists crucial to its ballistic missile program, but satellite images showed that the entire site—a sprawling complex composed of more than a dozen large buildings and other large structures—was essentially leveled by the blast.[31]

---

[28] James Risen, *State of War: The Secret History of the CIA and the Bush Administration* (New York: Free Press, 2006), chapter 9.

[29] Quoted in Eli Lake, "Operation Sabotage," *The New Republic*, July 14, 2010, http://www.tnr.com/article/world/75952/operation-sabotage?page=0,1

[30] See David Albright, *Peddling Peril: How the Secret Nuclear Trade Arms America's Enemies* (New York: Free Press, 2010), chapter 6; Collins and Frantz, *Fallout*, chapter 1. See also William J. Broad and David E. Sanger, "C.I.A. Secrets Could Surface in Swiss Nuclear Case," *New York Times*, December 23, 2010.

[31] David E. Sanger and William J. Broad, "Explosion Seen as Big Setback to Iran's Missile Program," *New York Times*, Dec 4, 2011.

The cause of the explosion, and whether it was an accident or an act of sabotage, is still unknown.[32] Iran quickly labeled the blast an accident, though subsequent discussions of the explosion in the Iranian news media referred to Moghaddam as a "martyr." Some Iranian officials even suggested that the base was hit by a missile from a CIA-operated drone. Years of sanctions may also have played a role in the blast. Iran struggles to acquire equipment and spare parts for its missile program, which can create dangerous working conditions.

A 2010 International Institute for Strategic Studies (IISS) report called Iran's development of solid-fuel missiles "a turning point" with "profound strategic implications."[33] If Iran fully harnesses this technology, it could allow it to produce long-range ballistic missiles. According to intelligence reports, the Shahab-3, Iran's most sophisticated ballistic missile, has a range of 1,250 miles, putting Israel within missile range. Solid-fuel missiles are easier to transport and hide than liquid-fuel missiles, making it more difficult for Israel or another country to destroy them in a pre-emptive attack. And unlike the more temperamental liquid-fuel missiles, solid-fuel missiles can be launched almost instantaneously. Iran has devoted much of its industrial resources to this type of missile in recent years, which theoretically could have intercontinental range someday.

How effective has this form of sabotage been? Sabotaging Iran's supply and procurements networks may have an indirect effect on slowing Iran's progress by forcing it to produce its own equipment and parts, which are often relatively low quality and prone to breakdowns. As a report by the Stimson Center stated:

> It is no secret that Iran's enrichment program has suffered from technical difficulties. While these difficulties may not all have been a direct result of sabotage, they are possible indirect consequences of it. If the Iranian government believes that nations are undertaking efforts to manipulate the components it procures, they may attempt to produce parts themselves. These in-house products would most likely be of lower quality than those produced abroad. Such faulty equipment could lead to the malfunctions and breakdowns Iran has experienced, delaying enrichment. The belief that Iran is the target of covert sabotage attempts also could lead the Iranian government to spend extra time closely inspecting all imported material...This would likewise delay the enrichment process.[34]

But while sabotage may cause delays and force a country to use greater caution and to expend greater resources acquiring material on the black market, both historically and in the case of Iran it has failed to cause prolonged disruptions to a country's nuclear program. Israel attempted to sabotage Iraq's quest for a nuclear reactor in the 1970s, but succeeded only in causing a brief delay in its construction. Iraq purchased the cores for its nuclear reactor from France, and in April 1979 Mossad operatives blew up a warehouse in the French port town of La Seyne-sur-Mer that was storing the cores, which were to be shipped imminently to the Tammuz-Osirak reactor just outside Baghdad.[35] The shipment was delayed for only six months while the cores were repaired, however. In 1981, when the reactor was set to go online, Israel destroyed it in a preventive military attack. The assault was intensely controversial, and rather than permanently crippling Iraq's nuclear program, Iraq instead accelerated its nuclear program and became even more determined to develop nuclear weapons.[36]

---

[32] American officials have said it was most likely an accident. Iran does not have much experience with what can be a highly volatile and dangerous technology. Even the United States has suffered accidents with solid-fuel motors.

[33] Mark Fitzpatrick, *Iran's Ballistic Missile Capabilities: A Net Assessment* (London: IISS, 2010).

[34] "Covert Operations in Iran," Stimson Center, December 30, 2010, http://www.stimson.org/spotlight/covert-operations-in-iran/

[35] Jeffrey Richelson, *Spying on the Bomb: American Nuclear Intelligence from Nazi Germany to Iran and North Korea* (New York: W.W. Norton, 2007), p. 321.

[36] See Dan Reiter, "Preventive Attacks against Nuclear Programs and the 'Success' at Osiraq," *The Nonproliferation Review* 12(2) (July 2005), pp. 355-371; Richard K. Betts, "The Osirak Fallacy," *National Interest* (Spring 2006), pp. 22-25; and Malfrid Braut-Hegghammer, "Revisiting Osirak: Preventive Attacks and Nuclear Proliferation Risks," *International Security* 36(1) (Summer 2011), pp. 101-132. On Israel's ability to strike Iran's nuclear facilities in a similar preventive attack, see Whitney Raas and Austin Long, "Osirak Redux? Assessing Israeli Capabilities to Destroy Iranian Nuclear Facilities," *International Security* 31(4) (Spring 2007), pp. 7-33.

Furthermore, Iran is increasingly able to machine many of the parts and equipment it needs for its nuclear program itself, which reduces its reliance on black market intermediaries and thus greatly diminishes its vulnerability to this kind of sabotage. As Iran's program becomes more sophisticated and indigenous, this form of sabotage will become increasingly ineffective.

Unleashing Cyber Attacks against Iran's Nuclear Infrastructure

A third strategy to disrupt Iran's enrichment program has been the use of cyber attacks on its nuclear infrastructure. The Stuxnet computer worm, a suspected joint American-Israeli project that was unleashed in early 2009, aimed to cause the centrifuges at the Natanz enrichment facility to malfunction and self-destruct. Computer software and security experts have called Stuxnet the most sophisticated and devastating cyber weapon ever deployed, with some even calling it unprecedented and revolutionary. Previous computer viruses, worms, and other malicious software (malware) typically infected Web sites or targeted corporate or military networks. Stuxnet was a different type of cyber attack, however. For the first time in history, a state sought to physically destroy the industrial infrastructure of another state by means of cyber attack.[37]

Of all the clandestine efforts to disrupt Iran's nuclear program, Stuxnet appears to have been the most successful, by some estimates delaying Iran's nuclear progress by one to two years.[38] The worm, which successfully breached Iran's most closely guarded state project, is believed to have been the cause of the apparent failure of nearly one-fifth of Iran's centrifuges in 2009 and 2010. It took Iranian officials months to determine the precise cause of the attack.

Its complexity and sophistication suggest that Stuxnet was a major government undertaking rather than the work of rogue computer hackers. Months, perhaps even years, of planning went into the attack. Only a government would have the time and resources to unleash such a weapon. While American and Israeli officials have refused to discuss the project publicly, there are only a few countries in the world that possess the means and the motive to launch an attack like Stuxnet.

Though Stuxnet infected computers in at least 155 countries, the outbreak was concentrated in Iran, suggesting it was the intended target. According to the computer security firm Symantec, nearly 60 percent of the infected computers worldwide were in Iran, 18 percent were in Indonesia, and eight percent were in India.[39] The worm infected more than 30,000 computers across Iran alone, including personal computers of scientists at the Natanz and Bushehr facilities.

Many intelligence agencies have come to see cyberwarfare as an irresistible allure because it is seemingly free of fingerprints. It is often extremely difficult to pinpoint the source of a cyber attack or the intended target with absolute certainty. The ubiquity and importance of computer systems and networks to modern life present both unlimited opportunities but also vulnerabilities for states. Complex computer networks control everything from military and economic activities, to telecommunications and critical infrastructure such as power plants and water systems.

Israel has built up a secretive cyberwarfare unit inside its intelligence service, and intelligence is the single biggest section of Israel's military. Unit 8200, the largest unit within Israeli intelligence, is devoted to signal, electronic, and computer network intelligence, and conducts secret cyberwar operations. The United States has built up its own cyberwarfare capability within the National Security Agency (NSA) and the military, in which the United States has recently opened a new Cyber Command. In recent years there has been a large increase in the sophistication of American cyberwarfare capabilities and the resources devoted to it.

---

[37] Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair*, April 2010.

[38] Because of its secretive nature, it is difficult to evaluate the damage Stuxnet caused to Iran's nuclear program with any precision. A confidential study making its way through U.S. national laboratories estimates that the worm slowed Iran's nuclear progress by one to two years. See David E. Sanger, "America's Deadly Dynamics with Iran," *New York Times*, November 5, 2011. There is no consensus among computer security experts and policy officials on how long the Stuxnet worm delayed Iran's nuclear progress, however.

[39] "A Worm in the Centrifuge," *Economist*, September 30, 2010. See also http://www.symantec.com/connect/blogs/w32stuxnet-network-information.

Planning and then implementing the Stuxnet attack was a huge technical and logistical challenge. The project reportedly began in the final months of the Bush administration. In January 2009, just before leaving office, Bush authorized a clandestine effort to sabotage the electrical and computer systems at Natanz. Israel reportedly tested the malicious code at its Dimona nuclear complex, where it managed to acquire P-1 centrifuges similar to the ones Iran was operating at Natanz. The United States also obtained P-1 centrifuges following the dismantlement of Libya's nuclear program, and these may also have been used to test the worm's effectiveness.[40]

Rather than seeking to cause as much havoc and destruction as possible, the Stuxnet worm was directed to infect a specific type of industrial control system made by Siemens, which was believed to be used at the Natanz enrichment site and at the Bushehr nuclear reactor.[41] The worm initially spread indiscriminately, but the specialized payload searched for specific Siemens software—WinCC, which runs on Microsoft Windows—that run industrial control systems. Computer security experts called it a marksman's job.[42] The worm spread throughout the computer network at Natanz, and possibly to other networks within Iran's nuclear and military apparatus. It exploited four previously unknown security holes in Windows (what computer security experts call "zero day vulnerabilities"), which was unprecedented. Once in the system the worm is almost impossible to dislodge and eradicate.[43]

Within these industrial control systems, the worm searched for the programmable logic controllers (PLC), which regulate machinery in everything from water and power plants, major construction and engineering projects, electrical power grids, oil pipelines, nuclear plants, and gas pipelines. In a nuclear facility, a PLC controls machinery such as the valves in centrifuges. The code stole design information to determine how best to sabotage the industrial control system, and then reprogrammed the PLC to send the centrifuges spinning wildly out of control.

The worm itself had two major components.[44] The first was to cause the centrifuges to spin wildly out of control. The code induced fluctuations in the rotational speed of the centrifuges' motors by taking over a power device known as a frequency converter. Rapid changes in the speed of these motors are a recipe for disaster. The centrifuges would spin so fast that the rotors would start to wobble uncontrollably and the machines would eventually destroy themselves. The Iranian IR-1 centrifuge normally spins at 1,064 Hertz (Hz), or cycles per second. The worm made the current hit 1,410 Hz for a full fifteen minutes, then returned to normal frequency. Twenty-seven days later, the worm took control of the centrifuges again, this time slowing the rotors down to a frequency of a few hundred Hz for a full 50 minutes.[45] By manipulating its speed, the rotor could crack, and even cause the centrifuge to explode.

The second function was to disguise the destruction that was taking place. The code produced fake, pre-recorded input data to circumvent digital safety systems and fool operators in the control room. To plant technicians, everything seemed to be normal, when in fact the centrifuges were destroying themselves. The worm was designed to give false industrial process control sensor signals (called a "man-in-the-middle" attack), which prevented any safety mechanisms from automatically kicking in, which would have shut the whole plant down before any destruction could occur.

---

[40] William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

[41] Western intelligence agencies had previously picked up that a shipment of these controllers was bound for Iran from Dubai, and that they were likely intended for Iran's nuclear program. Officials in Dubai seized the shipment before it could be sent to Iran.

[42] To protect it from viruses and other malware, the computer system at Natanz is not connected to the Internet. To initiate the attack, therefore, someone with direct access to the system had to plug an infected USB drive into one of the facility's computers.

[43] David E. Sanger, "Iran Fights Malware Attacking Computers," *New York Times*, September 25, 2010; William J. Broad and David E. Sanger, "Worm Was Perfect for Sabotaging Centrifuges," *New York Times*, November 18, 2010.

[44] John Markoff, "Worm Can Deal Double Blow to Nuclear Program," *New York Times*, November 19, 2010.

[45] Holger Stark, "Stuxnet Virus Opens New Era of Cyber War," *Spiegel Online*, August 8, 2011, http://www.spiegel.de/international/world/0,1518,778912,00.html.

There has been much debate over whether Stuxnet should be considered a success. To some, for all its renown and mystique, it was an operational and strategic failure. The Iranians discovered the worm, which was a serious blow to whoever perpetrated the attack. Iran now knows how foreign governments might try to sabotage its nuclear program through cyber attacks, as well as its computer networks' potential vulnerabilities. The element of surprise is now gone, and a potentially useful method of disrupting or even crippling Iran's nuclear program has been exposed. In response, Iran has taken steps to better protect its computer networks and to prevent successful cyber attacks in the future.

The designers could not control for unintended spillover, which shows one of the inherent dangers of cyber attacks. The Stuxnet worm affected innocent people, countries, companies, and institutions around the world, infecting tens of thousands of computer systems, from China, to India, Indonesia, Australia, Britain, and even the United States. As John Markoff, longtime technology writer for the *New York Times*, says, "If Stuxnet is the latest example of what a government organization can do, it contains some glaring shortcomings."[46]

Worst of all, while Stuxnet knocked out some of Iran's centrifuges, it did no lasting damage to Iran's nuclear program. It failed to cause a lengthy shutdown of Iran's enrichment program, let alone permanently disable it.[47] It took Iran only a few months to fully recover from the attack. According to nuclear inspectors, while some of the centrifuges were affected, the vast majority went unscathed. While Stuxnet may have succeeded in its tactical objective of knocking out some of Iran's centrifuges, it failed as a long-term strategic goal to substantially delay Iran's nuclear progress. According to IAEA inspectors, Iran now has the more advanced and efficient second-generation IR-2 centrifuge in operation, which are equipped with carbon fiber rotors and that operate at much higher speeds—up to 1,400 Hertz. The IR-2 centrifuges would likely be impervious to the existing version of the Stuxnet worm.

Most alarmingly, Stuxnet may have opened up a Pandora's box, legitimating a new form of cyberwarfare, for which the United States is acutely vulnerable.[48] Some of America's key infrastructure, such as power and water plants, electrical grids, chemical plants, oil refineries, and telecommunications networks are vulnerable to cyber attacks, and Stuxnet is a blueprint for waging industrial sabotage via cyber attack. The Stuxnet code was generic, which is perhaps the most dangerous and frightening element of the entire attack. That is, the code did not having anything specifically to do with centrifuges or uranium enrichment; it would work just as well if directed against a power or chemical plant. The code is now freely available on the Internet, and can be copied and modified easily. Some computer security experts have called Stuxnet a "cyber weapon of mass destruction" for its potential ability to wreak havoc on vital civilian infrastructure. Stuxnet therefore bought little time and security at great potential cost.[49]

How Effective Has the Covert Campaign Been?

In light of the above analysis, what conclusions can be drawn regarding covert action's ability to significantly slow down Iran's nuclear progress? Does covert action hold the promise of producing lasting setbacks to Iran's nuclear program, or is its impact limited and even counterproductive?

Years of sabotage and covert action have likely taken some psychological toll on Iranian officials. Speaking of efforts to infiltrate Iran's procurement networks, Bruce Riedel says, "One of the benefits of these kinds of programs is that over time it builds paranoia and fear inside the Iranian

---

[46] John Markoff, "A Silent Attack, but Not a Subtle One," *New York Times*, September 26, 2010.

[47] David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report, ISIS Reports, February 15, 2011, http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/

[48] Indeed, cyberwar is the ultimate in asymmetric warfare. See Joel Brenner, *American the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin, 2011).

[49] Stuxnet likely was not the last time the United States or Israel employed cyber attacks against Iran's nuclear program. It is not even clear if the original attack is over. Malicious code can lie dormant for long periods of time and then suddenly strike. A new Trojan horse program, called Duqu, appeared in late 2011. See John Markoff, "New Malicious Program by Creators of Stuxnet Is Suspected," *New York Times*, Oct 18, 2011.

nuclear program—that they have to be extremely careful that anything they buy may turn out to be a self-destructive pill once it's ingested inside the Iranian program."[50] Similarly, the attackers have demonstrated the ability to set off explosions throughout the country; kill some of Iran's most prominent nuclear scientists in brazen daylight attacks in the heart of Tehran; infect Iran's computer systems with harmful computer worms; and penetrate one of Iran's most closely guarded state secrets.

Despite this psychological toll, and the tactical success of individual operations—the long-term value of which is dubious—the risks and potential costs of covert action outweigh any potential benefits. There are at least three compelling rationales against the continued use of covert action against Iran's nuclear program. These include (1) its limited effectiveness at creating disruptions long enough for diplomacy or sanctions to work; (2) the propensity for retaliation and other acts of retribution, with the corresponding risk of uncontrolled escalation; and (3) making future diplomacy and a possible compromise much more difficult by hardening mutual suspicions and antagonisms. In sum, contrary to its advocates' claim that covert action will push back Iran's nuclear timetable, giving time for diplomacy to work, covert action will make diplomacy and compromise more difficult to achieve, not easier.

It is unlikely that covert action will be able to produce meaningful disruptions or delays to Iran's nuclear program—let alone permanently cripple it. Iran continues to steadily increase its stockpile of low-enriched uranium (LEU), producing 140 to 160 kilograms of uranium enriched to 3 to 5 percent per month, and, since February 2010, smaller quantities enriched to 20 percent. Iran's stockpile of LEU is now thought to be enough, with further enrichment, for five nuclear weapons.[51] In February 2012, Iran opened a second enrichment facility, named Fordo, where it has installed more advanced and efficient second-generation centrifuges. This facility is located on a Revolutionary Guards military base, under 250 feet of granite, and ringed by anti-aircraft guns, making it virtually impervious to airstrikes.

By now Iran has largely mastered the technology for uranium enrichment. If there were a time when Iran's enrichment program might have been vulnerable to sabotage and clandestine activity, that time has passed. It is possible that Iran's nuclear program would be even more advanced than it is now in the absence of covert action. Iran has had a nuclear program for nearly three decades, however, and the progress it has made in the past several years—during the height of the United States' and Israel's covert war against it—has, for Iran, been historically unprecedented.

Second, apart from covert actions' limited effectiveness, it could lead to Iranian retaliation against U.S. assets, interests, or allies in the Middle East, or perhaps even within the United States itself.[52] Covert action carries a high risk of "blowback," with the United States potentially facing acts of retribution around the world.[53] Because of its close association with Israel, moreover, the United States is likely to be held indirectly responsible for anything it does.[54] And the more active and visible the covert campaign becomes, the greater the affront to Iranian national prestige and sovereignty and the greater the likelihood of Iranian retaliation. This climate of insecurity, as Ali Vaez and Charles D. Ferguson of the Federation of American Scientists argue, "feeds ammunition to hardliners in Tehran

---

[50] Quoted in Mike Shuster, "Inside the United States' Secret Sabotage of Iran," *NPR*, May 9, 2011, http://www.npr.org/2011/05/09/135854490/inside-the-united-states-secret-sabotage-of-iran.

[51] Iran would need between three and twelve months to convert its stock of LEU to weapons-grade.

[52] Barbara Slavin, "Worries Mount over Blowback of Israeli Attack on Iran," *IPS*, January 18, 2012, http://ipsnews.net/news.asp?idnews=106478. In January 2012 the Obama administration's top intelligence official testified before Congress that Iranian leaders are now more willing to carry out attacks inside the United States. See Eric Schmitt, "Intelligence Report Lists Iran and Cyberattacks as Leading Concerns," *New York Times*, January 31, 2012. The bizarre assassination plot against the Saudi ambassador to the United States could be a foretaste, though Iranian complicity is debated. See Scott Shane and Artin Afkhami, "Allegations of Iranian and U.S. Plots Are Added to a History of Hostility," *New York Times*, Oct 14, 2011.

[53] On "blowback," see Chalmers Johnson, *Blowback: The Costs and Consequences of American Empire* (New York: Henry Holt, 2000).

[54] Thom Shanker, Helene Cooper, and Ethan Bronner, "U.S. Sees Iran Attacks as Likely if Israel Strikes," *New York Times*, February 29, 2012.

demanding reprisals."[55] Because of the United States' overwhelming military advantage, Iran would try to avoid a direct military confrontation. Instead, Iran would retaliate against U.S. assets and interests just enough to inflict harm but prevent a full-scale American military response.

Iran has shown it is highly adept at covert action and asymmetric warfare. Iran's Quds Force, an elite unit within the Revolutionary Guards, is capable of various forms of retaliation. The Quds Force was behind the 1996 truck bomb attack on the Khobar Towers housing complex in Saudi Arabia that killed 19 U.S. servicemen. Iran could also rely on proxy groups such as Hezbollah and Islamic Jihad to retaliate. Iran could strike at oil fields in Iraq, Kuwait, or Saudi Arabia, attack oil tankers in the Persian Gulf, or even close the Strait of Hormuz, a vital oil route, which would send oil prices soaring. And as RAND's Seth Jones reports, for the past decade Iran has provided refuge to some of al Qaeda's most senior leaders. Despite ideological and religious differences, the clerical regime and al Qaeda share a hatred of the United States and Israel, and Iran could unleash al Qaeda to retaliate against the United States or Israel.[56]

The United States and Israel therefore may ultimately be unleashing forces they will not fully be able to control. Through miscalculation or misperceptions, a clandestine, low-level covert campaign—along with the constant drumbeat of war coming from Israel and some in the United States—could escalate and lead to an unwanted military confrontation. In crises, as we know from history, the participants are never fully in control of events. If Iran retaliates against Israel, for example, Israeli leaders may use that as a *casus belli* and pretext for a wider and more sustained military response. And as Iran gets closer to a nuclear weapons capability, the United States and/or Israel could wage bigger, bolder, and riskier covert operations in a vain attempt to forestall Iran's progress, which would move the confrontation from a "virtual" to an actual state of war.

Additionally, the United States may be setting a dangerous precedent with its covert war against Iran. The rest of the world, especially China and Russia, is surely watching events inside Iran. If other states decide to interfere in the internal affairs of their perceived enemies to the degree the United States and Israel have allegedly interfered in Iran's internal affairs, the world will be much more chaotic, unstable, and disorderly.

Finally, and most importantly, because it cuts to the heart of the strategic rationale its advocates use, covert action is making future diplomacy and compromise with Iran more difficult. It is hard to negotiate with a country if it is convinced you are killing its scientists, blowing up its military bases, and unleashing vicious cyber attacks against its industrial infrastructure.

The relationship between Washington and Tehran is already characterized by a high degree of mutual mistrust, suspicion, and hostility. For many in the United States, the regime in Tehran is the ultimate illiberal enemy. For Tehran, the United States is intent on crippling and ultimately overthrowing the regime. The covert campaign only serves to reinforce these images.[57] Iranians are now likely to suspect the United States and Israel for any suspicious accident or mishap related to its nuclear or military programs.

This points to a bigger problem that the core assumptions on which covert action's strategic rational is based have not been appropriately examined. The core logic for covert action's supposed effectiveness is as follows: (1) covert action will disrupt and delay Iran's nuclear progress for an amount of time sufficient to enable sanctions and diplomacy to work; (2) Iran will be more open to reach a compromise to resolve the nuclear crisis; and (3) the benefits of covert action outweigh any potential costs and risks. This analysis has shown, however, that the covert campaign has failed to appreciably set back Iran's nuclear progress. By hardening mutual suspicion and antagonism, covert action makes diplomacy more difficult, strengthens Iran's resolve, and raises the domestic political costs of being seen to back down. The costs and risks of covert action—the propensity for Iranian retaliation, the risk of escalation, weakening international norms against assassination and cyber

---

[55] Quoted in Maclean, "Not-So-Covert War in Iran Buys Time But Raises Tension."

[56] Seth G. Jones, *Hunting in the Shadows: The Pursuit of al Qa'ida since 9/11* (New York: W.W. Norton, 2012).

[57] I thank Stefano Recchia for this point. On how America's Liberal political cultural tends to distort threats, see Michael C. Desch, "Liberalism and the New Definition of Existential Threat," in Oren Barak and Gabriel Sheffer, eds., *Existential Threats and Civil-Security Relations* (Lanham, Md.: Lexington Books, 2009), pp. 37-60.

warfare—outweigh any possible benefits. And while harsher economic sanctions have accompanied the covert campaign, a parallel diplomatic strategy has not. This further shows that the covert campaign is more an act of desperation rather than one element in a well-conceived strategic approach toward Iran's nuclear program.

The covert war is thus largely self-defeating and counterproductive. To deter what it perceives to be American and Israeli aggression, the regime in Tehran could become even more determined to attain a nuclear weapons capability. A 2011 RAND report argued that covert action might have "the unintended consequence of fortifying the regime's resolve in continuing the nuclear program."[58] As longtime Iran observer Gary Sick puts it, if the tables were turned, and a foreign government were killing American scientists, sabotaging our critical infrastructure, and unleashing destructive computer viruses into our country, we would be enraged. Covert action, along with increasingly severe economic sanctions, may drive Iran, in an act of defiance or desperation, to do precisely what we are trying to prevent them to do: build nuclear weapons.

Conclusion

In the near term, as Iran seems to move inexorably toward acquiring a nuclear weapons capability, a continuation and perhaps even an escalation of covert operations seems possible. But as this analysis has shown, covert action is hardly the silver bullet that will prevent Iran from developing nuclear weapons and resolve the nuclear crisis. The ostensible benefits of covert action are largely illusory, they often have consequences far different to those that were anticipated or expected, and they will make a future compromise more difficult. In sum, there is little persuasive strategic or political rationale for continuing the covert campaign.

Two implications therefore follow from this analysis. The first is that covert action against Iran should be substantially reduced, if not suspended entirely. The second is that alternative strategies must be pursued more vigorously. Despite offering a diplomatic gesture to Tehran early in his term, Obama has largely eschewed the diplomatic option.[59] This has been a mistake. Comprehensive negotiations with Tehran over the magnitude, scope, and nature of its nuclear program are badly needed. In addition, to escape from the vicious circle in which the Americans, Israelis, and Iranians are trapped, the United States should include a pledge that it does not seek the overthrow of the regime in Tehran.[60] A lasting solution can hardly be assured if such actions are taken, and the political challenges will be significant, but such negotiations may be the last chance to prevent Iran from developing nuclear weapons and letting the crisis continue indefinitely, with the risks that entails.

This analysis also raises important ethical as well as strategic questions related to the role of covert action in statecraft and national security policy. Where should states draw the line between legitimate actions to defend themselves, their interests, or their values, and actions that may violate or compromise these very ideals? Israeli leaders, for example, consider (or at least publicly claims) that Iran poses an existential threat to the state of Israel and even to the future of the Jewish people. When such stakes are involved, some argue, hidden and at times ruthless tactics are justified. Rather than a fixed boundary, however, the frontier between our security and interests and where our core principles lie is always shifting. The dictates of covert warfare at times seek to define this boundary for us. Future administrations will surely see covert action as an at times necessary and expedient instrument of statecraft, but they should resist this temptation, especially in the context of counterproliferation.

---

[58] James Dobbins, Alireza Nader, Dalia Dassa Kaye, and Frederic Wehrey, *Coping with a Nuclearizing Iran* (Santa Monica, Calif.: RAND Corporation, 2011), p. 86.

[59] Trita Parsi, *A Single Roll of the Dice: Obama's Diplomacy with Iran* (New Haven, Conn.: Yale University Press, 2012).

[60] Martin Indyk, "Iran Spinning Out of Control," *New York Times*, February 29, 2012.


European
University
Institute
European University Press