<p><br />Abridged by Alex Shone , Research Associate in Residence, U K Defence Forum, from an article, originally published by the New York Times on January 15th 2011, written by William J Broad, John Markoff and David E Sanger<br /><br />The Dimona complex in the Negev desert is famous as the heavily guarded heart of Israel's never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal. Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role � as a critical testing ground in a joint American and Israeli effort to undermine Iran's efforts to make a bomb of its own. They say Dimona tested the effectiveness of the Stuxnet computer worm, a destructive programme that appears to have wiped out roughly a fifth of Iran's nuclear centrifuges and helped delay, though not destroy, Tehran's ability to make its first nuclear arms.<br /><br />Many mysteries remain, chief among them, exactly who constructed a computer worm that appears to have several authors on several continents. In early 2008 the German company Siemens cooperated with one of the United States' premier national laboratories, in Idaho, to identify the vulnerabilities of computer controllers that the company sells to operate industrial machinery around the world � and that American intelligence agencies have identified as key equipment in Iran's enrichment facilities.<br /><br />The worm itself now appears to have included two major components. One was designed to send Iran's nuclear centrifuges spinning wildly out of control. Another seems right out of the movies: The computer programme also secretly recorded what normal operations at the nuclear plant looked like, then played those readings back to plant operators, like a pre-recorded security tape in a bank heist, so that it would appear that everything was operating normally while the centrifuges were actually tearing themselves apart. The attacks were not fully successful: Some parts of Iran's operations ground to a halt, while others survived, according to the reports of international nuclear inspectors. Nor is it clear the attacks are over: Some experts who have examined the code believe it contains the seeds for yet more versions and assaults.<br /><br />Officially, neither American nor Israeli officials will even utter the name of the malicious computer programme; much less describe any role in designing it. But Israeli officials grin widely when asked about its effects. In recent days, American officials who spoke on the condition of anonymity have said in interviews that they believe Iran's setbacks have been underreported. The project's political origins can be found in the last months of the Bush administration. President Obama, first briefed on the programme even before taking office, sped it up, according to officials familiar with the administration's Iran strategy. Israel has long been seeking a way to cripple Iran's capability without triggering the opprobrium, or the war, that might follow an overt military strike of the kind they conducted against nuclear facilities in Iraq in<br />Perhaps the most secretive part of the Stuxnet story centres on how the theory of cyber-destruction was tested on enrichment machines to make sure the malicious software did its intended job. The account starts in the Netherlands. In the 1970s, the Dutch designed a tall, thin machine for enriching uranium. As is well known, A. Q. Khan, a Pakistani metallurgist working for the Dutch, stole the design and in 1976 fled to Pakistan. The resulting machine, known as the P-1, for Pakistan's first-generation centrifuge, helped the country get the bomb. And when Dr. Khan later founded an atomic black market, he illegally sold P-1's to Iran, Libya, and North Korea.<br /><br />How and when Israel obtained this kind of first-generation centrifuge remains unclear, whether from Europe, or the Khan network, or by other means. But nuclear experts agree that Dimona came to hold row upon row of spinning centrifuges. By early 2004, a variety of federal and private nuclear experts assembled by the Central Intelligence Agency were calling for the United States to build a

secret plant where scientists could set up the P-1's and study their vulnerabilities. The resulting plant, nuclear experts said last week, may also have played a role in Stuxnet testing.<br /><br />In November, the Iranian president, Mahmoud Ahmadinejad, broke the country's silence about the worm's impact on its enrichment programme, saying a cyber attack had caused "minor problems with some of our centrifuges." Fortunately, he added, "our experts discovered it." The most detailed portrait of the damage comes from the Institute for Science and International Security, a private group in Washington. Last month, it issued a lengthy Stuxnet report that said Iran's P-1 machines at Natanz suffered a series of failures in mid- to late 2009 that culminated in technicians taking 984 machines out of action. The report called the failures "a major problem" and identified Stuxnet as the likely culprit.<br /><br />Stuxnet is not the only blow to Iran. Sanctions have hurt its effort to build more advanced (and less temperamental) centrifuges. And last January, and again in November, two scientists who were believed to be central to the nuclear program were killed in Tehran. The man widely believed to be responsible for much of Iran's programme, Mohsen Fakrizadeh, a college professor, has been hidden away by the Iranians, who know he is high on the target list. Publicly, Israeli officials make no explicit ties between Stuxnet and Iran's problems. But in recent weeks, they have given revised and surprisingly upbeat assessments of Tehran's nuclear status.</p>