2 November 2011 Last updated at 10:28 GMT

Israeli army tests rocket system

Israel has tested a rocket propulsion system from a military base in the centre of the country, the defence ministry said.

Israeli media reports said a ballistic missile had been fired.

The test came amid speculation in Israel that the government could be preparing a military strike against Iran's nuclear facilities.

The defence ministry said the test had long been planned. Israel successfully tested a ballistic missile in 2008.

"Israel today carried out the test of a rocket propulsion system from the Palmachim base," near Rishon LeZion, a military statement said.

"This had been planned by the defence establishment a long time ago and was carried out as scheduled".

The statement gave no details on what type of rocket had been tested, but Israel's Haaretz newspaper said a new type of ballistic missile was being tested.

A trail of white smoke could be seen across large areas of central Israel, newspapers reported.

Haaretz reported on Wednesday that Prime Minister Benjamin Netanyahu had been trying to persuade his cabinet to back military action against Iran.

Israel and Western powers say Iran has been trying to build a nuclear weapon. Iran says its nuclear programme is for peaceful purposes.

UK military steps up plans for Iran attack amid fresh nuclear fears

British officials consider contingency options to back up a possible US action as fears mount over Tehran's capability

- Nick Hopkins
- guardian.co.uk, Wednesday 2 November 2011 15.21 GMT

Iranian nuclear technicians in protective wear. Photograph: Mehdi Ghasemi/AP

Britain's armed forces are stepping up their contingency planning for potential military action against Iran amid mounting concern about Tehran's nuclear enrichment programme, the Guardian has learned.

The Ministry of Defence believes the US may decide to fast-forward plans for targeted missile strikes at some key Iranian facilities. British officials say that if Washington presses ahead it will seek, and receive, UK military help for any mission, despite some deep reservations within the coalition government.

In anticipation of a potential attack, British military planners are examining where best to deploy Royal Navy ships and submarines equipped with Tomahawk cruise missiles over the coming months as part of what would be an air and sea campaign.

They also believe the US would ask permission to launch attacks from Diego Garcia, the British Indian ocean territory, which the Americans have used previously for conflicts in the Middle East.

The Guardian has spoken to a number of Whitehall and defence officials over recent weeks who said Iran was once again becoming the focus of diplomatic concern after the revolution in Libya.

They made clear that Barack Obama, has no wish to embark on a new and provocative military venture before next November's presidential election.

But they warned the calculations could change because of mounting anxiety over intelligence

gathered by western agencies, and the more belligerent posture that Iran appears to have been taking.

Hawks in the US are likely to seize on next week's report from the International Atomic Energy Agency, which is expected to provide fresh evidence of a possible nuclear weapons programme in Iran.

The Guardian has been told that the IAEA's bulletin could be "a game changer" which will provide unprecedented details of the research and experiments being undertaken by the regime.

One senior Whitehall official said Iran had proved "surprisingly resilient" in the face of sanctions, and sophisticated attempts by the west to cripple its nuclear enrichment programme had been less successful than first thought.

He said Iran appeared to be "newly aggressive, and we are not quite sure why", citing three recent assassination plots on foreign soil that the intelligence agencies say were coordinated by elements in Tehran.

In addition to that, officials now believe Iran has restored all the capability it lost in a sophisticated cyber-attack last year.The Stuxnet computer worm, thought to have been engineered by the Americans and Israelis, sabotaged many of the centrifuges the Iranians were using to enrich uranium.

Up to half of Iran's centrifuges were disabled by Stuxnet or were thought too unreliable to work, but diplomats believe this capability has now been recovered, and the IAEA believes it may even be increasing.

Ministers have also been told that the Iranians have been moving some more efficient centrifuges into the heavily-fortified military base dug beneath a mountain near the city of Qom.

The concern is that the centrifuges, which can be used to enrich uranium for use in weapons, are now so well protected within the site that missile strikes may not be able to reach them. The senior Whitehall source said the Iranians appeared to be shielding "material and capability" inside the base.

Another Whitehall official, with knowledge of Britain's military planning, said that within the next 12 months Iran may have hidden all the material it needs to continue a covert weapons programme inside fortified bunkers. He said this had necessitated the UK's planning being taken to a new level.

"Beyond [12 months], we couldn't be sure our missiles could reach them," the source said. "So the window is closing, and the UK needs to do some sensible forward planning. The US could do this on their own but they won't.

"So we need to anticipate being asked to contribute. We had thought this would wait until after the US election next year, but now we are not so sure.

"President Obama has a big decision to make in the coming months because he won't want to do anything just before an election."

Another source added there was "no acceleration towards military action by the US, but that could change". Next spring could be a key decision-making period, the source said. The MoD

has a specific team considering the military options against Iran.

The Guardian has been told that planners expect any campaign to be predominantly waged from the air, with some naval involvement, using missiles such as the Tomahawks, which have a range of 800 miles (1,287 km). There are no plans for a ground invasion, but "a small number of special forces" may be needed on the ground, too.

The RAF could also provide air-to-air refuelling and some surveillance capability, should they be required. British officials say any assistance would be cosmetic: the US could act on its own but would prefer not to.

An MoD spokesman said: "The British government believes that a dual track strategy of pressure and engagement is the best approach to address the threat from Iran's nuclear programme and avoid regional conflict. We want a negotiated solution – but all options should be kept on the table."

The MoD says there are no hard and fast blueprints for conflict but insiders concede that preparations there and at the Foreign Office have been under way for some time.

One official said: "I think that it is fair to say that the MoD is constantly making plans for all manner of international situations. Some areas are of more concern than others. "It is not beyond the realms of possibility that people at the MoD are thinking about what we might do should something happen on Iran. It is quite likely that there will be people in the building who have thought about what we would do if commanders came to us and asked us if we could support the US. The context for that is straightforward contingency planning."

Washington has been warned by Israel against leaving any military action until it is too late.

Western intelligence agencies say Israel will demand that the US act if it believes its own military cannot launch successful attacks to stall Iran's nuclear programme. A source said the "Israelis want to believe that they can take this stuff out", and will continue to agitate for military action if Iran continues to play hide and seek.

It is estimated that Iran, which has consistently said it is interested only in developing a civilian nuclear energy programme, already has enough enriched uranium for between two and four nuclear weapons.

Experts believe it could be another two years before Tehran has a ballistic missile delivery system.

British officials admit to being perplexed by what they regard as Iran's new aggressiveness, saying that they have been shown convincing evidence that Iran was behind the murder of a Saudi diplomat in Karachi in May, as well as the audacious plot to assassinate the Saudi ambassador in Washington, which was uncovered last month.

"There is a clear dotted line from Tehran to the plot in Washington," said one.

Earlier this year, the IAEA reported that it had evidence Tehran had conducted work on a highly sophisticated nuclear triggering technology that could only be used for setting off a nuclear device.

It also said it was "increasingly concerned about the possible existence in Iran of past or current

undisclosed nuclear-related activities involving military-related organisations, including activities related to the development of a nuclear payload for a missile."

Last year, the UN security council imposed a fourth round of sanctions on Iran to try to deter Tehran from pursuing any nuclear ambitions.

At the weekend, the New York Times reported that the US was looking to build up its military presence in the region, with one eye on Iran.

According to the paper, the US is considering sending more naval warships to the area, and is seeking to expand military ties with the six countries in the Gulf Co-operation Council: Saudi Arabia, Kuwait, Bahrain, Qatar, the United Arab Emirates and Oman.

Tony Blair: West should use force if Iran 'continues to develop nuclear weapons'

Former prime minister says it is wholly unacceptable for Tehran to seek nuclear weapons capability

- Mark Tran
- guardian.co.uk, Wednesday 1 September 2010 11.25 BST

A 2007 satellite image of Iran's Natanz uranium enrichment facility. Photograph: GeoEye/AP

The west should use force against Iran if it "continues to develop nuclear weapons", Tony Blair said today, aligning himself with US hawks who have called for strikes against Iranian nuclear sites.

The former prime minister made his comments in a BBC interview to publicise his memoirs, A

Journey, which are published today.

Blair said it was "wholly unacceptable" for Tehran to seek a nuclear weapons capability and insisted there could be "no alternative" to military force "if they continue to develop nuclear weapons".

Speaking to Andrew Marr in a BBC interview to be broadcast tonight, Blair says: "I am saying that I think it is wholly unacceptable for Iran to have a nuclear weapons capability and I think we have got to be prepared to confront them, if necessary militarily. I think there is no alternative to that if they continue to develop nuclear weapons. They need to get that message loud and clear."

Iran is enriching uranium at its main, internationally-monitored plant at Natanz and is building a second enrichment facility run by the Revolutionary Guards inside a mountain at Fordo, near Qom, southwest of Tehran. Enriched uranium can be used as fuel to power nuclear reactors as well as to make the fissile core of an atom bomb.

Tehran insists its nuclear activities are purely peaceful and argues that as a signatory to the Nuclear Non-Proliferation Treaty (NPT) it has the right to peaceful nuclear technology. But the UN last month imposed a fourth round of sanctions on Iran because of fears it may be secretly developing nuclear weapons.

The US and Israel – an undeclared nuclear power outside the NPT – have both refused to rule out military action against Iran.

In his exclusive interview with the Guardian, Blair elaborates on why it is unacceptable for Iran to have nuclear weapons, linking this to the 9/11 attacks on the US. The former prime minister wishes he had seen earlier that 9/11 had "far deeper roots" than he thought at the time.

"The reason for that, let me explain it, is that in my view what was shocking about September 11 was that it was 3,000 people killed in one day but it would have been 300,000 if they could have done it," Blair said, appearing to equate al-Qaida with Iran. "That's the point ... I decided at that point that you cannot take a risk on this. This is why I am afraid, in relation to Iran, that I would not take a risk of them getting nuclear weapons capability. I wouldn't take it.

"Now other people may say: 'Come on, the consequences of taking them on are too great, you've got to be so very careful, you'll simply upset everybody, you'll destabilise it.' I understand all of those arguments. But I wouldn't take the risk of Iran with a nuclear weapon."

In the postscript to his book, Blair writes: "Iran with a nuclear bomb would mean others in the region acquiring the same capability; it would dramatically alter the balance of power in the region, but also within Islam."

Blair's approach to Iran aligns him with US hawks such as John Bolton, the former American ambassador to the UN, who believes that Israel should have attacked Iran before it started loading fuel into its first nuclear power plant in the southern port city of Bushehr on 21 August, although nuclear experts say Bushehr has no link with Iran's secretive uranium enrichment programme, seen as the main "weaponisation" threat, at other installations.

2 September 2011 Last updated at 16:47 GMT

UN 'growing concern' over Iran nuclear weapons plan

Iran insists its nuclear programme is for peaceful purposes

The UN nuclear watchdog says it is "increasingly concerned" that Iran is secretly working on components for a nuclear weapons programme.

The International Atomic Energy Agency (IAEA) describes its information as "extensive and comprehensive".

In a report seen by news agencies, it also says Tehran is preparing to enrich uranium at a new location - an underground bunker near Qom.

Tehran insists its nuclear programme is entirely peaceful.

Iran is subject to UN Security Council sanctions for refusing to freeze its enrichment programme.

Uranium enrichment can produce fuel for a nuclear reactor but can also be used to make a nuclear warhead.

'Undisclosed' activities?
The IAEA says "many member states" had provided evidence for its latest assessment on Iran's nuclear ambitions.

Extracts of the report, published by the AFP news agency, said the IAEA was "increasingly concerned about the possible existence in Iran of past or current undisclosed nuclear related activities involving military related organisations".

These included "activities related to the development of a nuclear payload for a missile".

The report adds that IAEA Director General Yukiya Amano wrote to Iran's nuclear chief Fereydoun Abbasi Davani in June and "reminded Iran that it should fully implement all its obligations in order to establish international confidence in the exclusivity peaceful nature of Iran's nuclear programme".

Iran has so far not responded to the report.

Six world powers are negotiating with Iran over its nuclear programme.

Iran concealed its enrichment programme for 18 years. The Security Council says that until

Iran's peaceful intentions can be fully established, it should stop enrichment and other nuclear activities.

The UN has so far slapped four rounds of sanctions on Iran; however, they do not block the trade in oil and gas, the major source of Iran's income.

Iran moves nuclear technology underground

US says transfer of centrifuges to an underground uranium enrichment site raises suspicions.

Last Modified: 23 Aug 2011 01:56

Fereidoun Abbasi said engineers are 'hard at work' preparing a new nuclear facility in Fordo [EPA]

Iran has moved some of its centrifuges to an underground uranium enrichment site that offers better protection from possible air strikes, the country's vice president said.

Engineers are "hard at work" preparing the facility in Fordo, which is carved into a mountain to protect it against possible attacks, to house the centrifuges, Fereidoun Abbasi was quoted as saying by state TV on Monday.

Abbasi, who is also Iran's nuclear chief, did not say how many centrifuges have been moved to Fordo nor whether the machines installed are the new, more efficient centrifuges Iran has promised or the old IR-1 types.

He did specify that the centrifuges will be taken to Fordo from Iran's main uranium enrichment facility in Natanz, central Iran.

Uranium enrichment lies at the heart of Iran's dispute with the West, a technology that can be used to produce nuclear fuel or materials for atomic bombs.

The United States and some of its allies accuse Iran of using its civilian nuclear program as a cover to develop atomic weapons. Iran has denied the charges, saying its nuclear program is peaceful and solely aimed at generating electricity.

On Monday, US State Department spokeswoman Victoria Nuland said the new programme raises suspicions.

"The Iranian nuclear programme offers no plausible reasons for its existing enrichment of uranium up to nearly 20 per cent, nor ramping up this production, nor moving centrifuges underground," she said. "And its failure to comply with its obligations to suspend its enrichment activities up to 3.5 per cent and nearly 20 per cent have given all of us in the international community reason to doubt its intentions."

Iran has been enriching uranium to less than five per cent for years, but it began to further

enrich its uranium stockpile to nearly 20 per cent as of February 2010, saying it needs the higher grade material to produce fuel for a Tehran reactor that makes medical radioisotopes for cancer treatment.

Weapons-grade uranium is usually about 90 per cent enriched.

Iran's higher-grade enrichment efforts are of particular concern to the West because uranium at 20 per cent enrichment can be converted into fissile material for a nuclear warhead much more quickly than that at 3.5 per cent.

Abbasi said Tehran was in no rush to install the centrifuges and that experts are observing all technical standards.

In June, Abbasi said Iran plans to triple its output of the 20 percent enriched uranium and move the entire program to the new, secretly-built Fordo facility, just north of the holy city of Qom in central Iran.

5 September 2011 Last updated at 15:39 GMT

Fake DigiNotar web certificate risk to Iranians

Iran was a heavy user of DigiNotar certificates around the time that fake certificates were created

Fresh evidence has emerged that stolen web security certificates may have been used to spy on people in Iran.

Analysis by Trend Micro suggests a spike in the number of compromised DigiNotar certificates being issued to the Islamic Republic.

It is believed the digital IDs were being used to trick computers into thinking they were directly accessing sites such as Google.

In reality, someone else may have been monitoring the communications.

Hundreds of bogus certificates are thought to have been generated following a hack on Netherlands-based DigiNotar.

The company is owned by US firm Vasco Data Security.

Web passport

Authentication certificates are used to verify secure websites' identity

Authentication certificates are used by many websites to give their users secure access.

Typically these take the form of a TLS or SSL connection - which can be identified by the appearance of a padlock logo and "https" prefix.

Together, they are supposed to guarantee that the site is what it appears to be, and that the user's session is not being monitored.

Hundreds of bodies - known as certificate authorities (CAs) - are allowed to provide such authentication.

Web browsers, such as Safari, Chrome, Firefox and Internet Explorer have a built-in list of which CAs they can trust.

However, if a third-party was able to steal certificate details or generate their own, they may be able to launch a "man-in-the-middle" attack, similar to tapping a phone line.

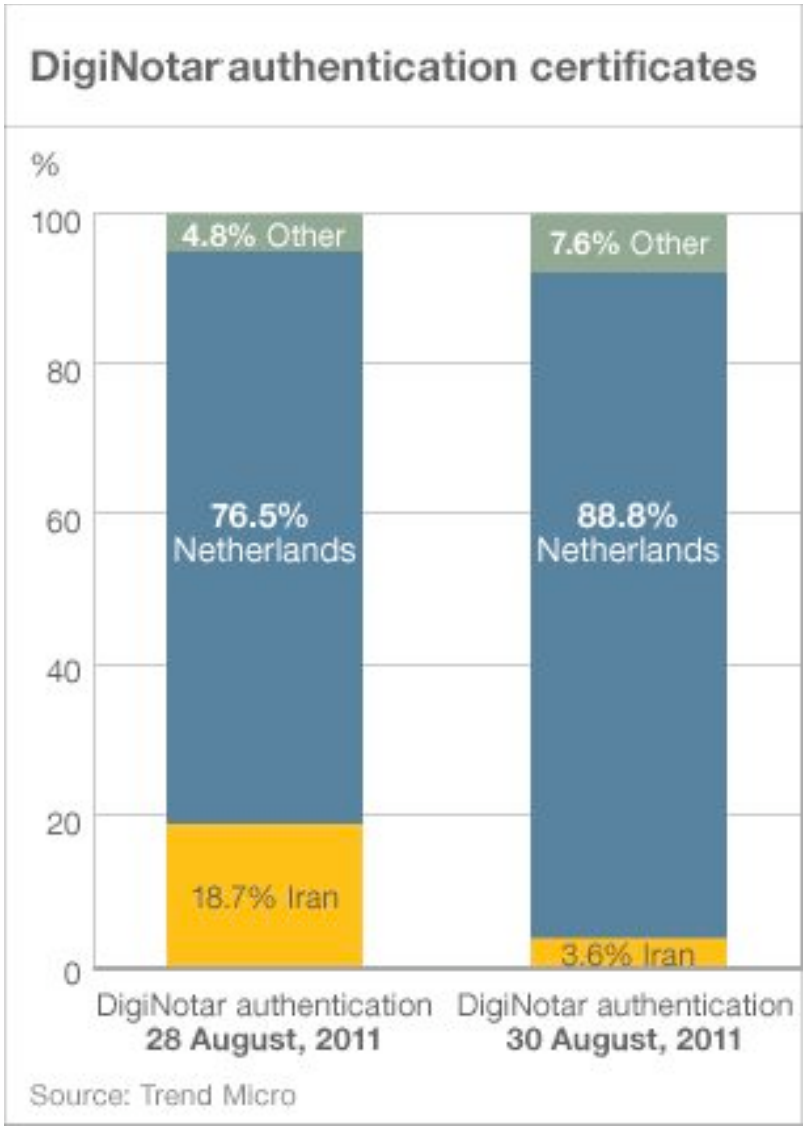
The presence of an apparently genuine certificate means browser security would be unlikely to detect the surveillance.

Issued and revoked

On 19 July, Dutch CA DigiNotar detected an unauthorised intrusion into its systems.

The company immediately revoked a number of bogus certificates that had been created as a result.

It emerged later that some were missed, and other new ones generated, after the initial attack.



Unconfirmed information published online suggested that more than 500 false DigiNotar certificates exist.

Among the domains listed are Google, Facebook, Twitter and Skype.

At the same time, it was noticed that a sizeable portion of the Dutch company's certificates were mysteriously going to users in Iran.

By August, 76.5% of DigiNotar validations were in the Netherlands. 18.7% were in Iran and 4.8% elsewhere in the world, according to security firm Trend Micro.

Iranian activity dropped off after the certificates were revoked.

DigiNotar eventually went public about the intrusion on 30 August, at which time most web browsers stopped recognising DigiNotar certificates altogether.

Soft target

There are many reasons why Iran may have been targeted using the bogus certificates, according to security experts.

The republic's tight controls on dissent mean that monitoring web traffic could yield useful

information.

Iran's internet setup also makes some types of interception easier, according to Rik Ferguson, Trend Micro's director of security research and communications.

"All the internet traffic has to go through an Iranian government proxy before it goes out to the final destination.

Continue reading the main story

The internet's most used Certificate Authorities

- Verisign
- GoDaddy
- Comodo
- Network Solutions
- Entrust
- GlobalSign
- AmbironTrustWave

Source: Netcraft

"If you want to spy on normal HTTP traffic, that is not a problem - you get to see all the outbound requests and all the inbound responses," he explained.

For secure websites, attempts to intercept would ring alarm bells with the web browser and therefore the user.

One option is to make the Iranian national proxy server look like it is the target website - using a fake DigiNotar certificate.

The proxy then relays information to and from the real website, e.g. Google.com, but there is no indication that the secure chain has been broken.

Government involvement?
While much online debate has centred around the role of the Iranian authorities, there is no firm evidence to support such a theory.

However, a spokesman for the Dutch Interior Ministry, Vincent van Steen told the Netherland's-based ANP news agency that the cabinet was looking into claims of Iranian government involvement.

Iran has previously been on the receiving end of cyber attacks, including the elaborate Stuxnet conspiracy which enabled a computer worm to take control of machinery in a uranium enrichment plant.

The DigiNotar incident has also raised broader concerns about the security of the global certificate authorisation system.

"The more there are, the more opportunities there are to attack the system," said Paul Mutton, a security analyst from Netcraft.

"Whenever there is a certificate authority that is trusted by all the mainstream web browsers, if

someone was to compromise them it is just as bad as compromising the largest CA."

Alternatives to the current system have been suggested, including one by former hacker Moxie Marlinspike, known as Convergence, which verifies site authenticity by checking with multiple online "notaries".

6 September 2011 Last updated at 10:45 GMT

Iranians hit in email hack attack

The fake certificates were used to snoop on messages sent via Google email

Up to 300,000 Iranians may have had their Google email monitored using security certificates stolen from Dutch firm DigiNotar.

The figure came from a report into the breach at DigiNotar which let attackers generate hundreds of fake certificates.

The report suggests the certificates were used in Iran to eavesdrop on email accounts.

The list has been passed to Google so it can tell victims they may have come under government scrutiny.

On 30 August, security firm Fox-IT was called in to analyse the sequence of events at DigiNotar that led to the security breach. It published its interim report late on 5 September.

DigiNotar is one of many firms which help to ensure that no-one is eavesdropping on secure communications between users and the sites they visit.

It does this via security certificates which act as a guarantee of identity so people can be sure they are connecting to the site they think they are.

Anyone armed with a rogue certificate for a web firm or service can impersonate that organisation and get at communications that would otherwise be impossible to read because they are encrypted.

"The network has been severely breached"
Fox-IT

DigiNotar first took action to revoke fake security certificates on 19 July when it found that hackers had got access to its internal network.

The Fox-IT report suggests that the hackers were able to access those internal systems for a month before DigiNotar took action.

The first exploration by the hackers took place on 6 June, suggests the report, and the first rogue certificates were issued on 10 July.

"The network has been severely breached," said the report. It said security procedures at DigiNotar were clearly lacking because the tools the hackers used and installed on network computers can be detected by standard anti-virus software.

All evidence gathered by Fox-IT suggests that the attacks were carried out to help surveillance of Iranian net users. More than 99% of the 300,000 IP addresses known to have connected to Google's email service with the help of a fake security certificate are in Iran.

Fox-IT noted that the use of the fake certificates would also have given attackers access to small text files known as cookies that Google and many others use to recognise regular visitors.

As a result, Fox-IT said: "It would be wise for all users in Iran to at least logout and login but even better change passwords."

DigiNotar has called on the Dutch government to help it recover following the attack. In its wake Google and many others have issued updates to ensure that the fake certificates are no longer recognised.

DigiNotar is the second security certificate firm to suffer at the hands of hackers. In March 2011, Comodo revealed that it had been hit and pointed the finger at Iran.

Now evidence is emerging that the same hackers were behind both attacks according to a message posted to the pastebin website. In the message, the hacker or hackers claim to have access to four other security certificate firms.

24 March 2011 Last updated at 11:18 GMT

Iran accused in 'dire' net security attack

The attack was run from servers based in Iran, suggests analysis

Hackers in Iran have been accused of trying to subvert one of the net's key security systems.

Analysis in the wake of the thwarted attack suggests it originated and was co-ordinated via servers in Iran.

If it had succeeded, the attackers would have been able to pass themselves off as web giants Google, Yahoo, Skype, Mozilla and Microsoft.

The impersonation would have let attackers trick web users into thinking they were accessing the real service.

Fake identity
The attack was mounted on the widely used online security system known as the Secure Sockets Layer or SSL.

This acts as a guarantee of identity so users can be confident that the site they are visiting is who it claims to be. The guarantee of identity is in the form of a digital passport known as a certificate.

Analysis of the attack reveals that someone got access to the computer systems of one firm that issue certificates. This allowed them to issue bogus certificates that, if they had been used, would have let them impersonate any one of several big net firms.

It appears that the attackers targeted the SSL certificates of several specific net communication services such as Gmail and Skype as well as other popular sites such as Microsoft Live, Yahoo and the Firefox browser.

SSL certificate issuer Comodo published an analysis of the attack which was carried out via the computer systems of one of its regional affiliates.

It said the attack exhibited "clinical accuracy" and that, along with other facets of the attack led it to one conclusion: "this was likely to be a state-driven attack."

It is thought it was carried out by the Iranian authorities to step up scrutiny of opposition groups in the country that use the web to co-ordinate their activity.

The bogus certificates have now been revoked and Comodo said it was looking into ways of improving security at its affiliates.

Browsers have also been updated so anyone visiting a site whose credentials are guaranteed by the bogus certificates will be warned.

Writing on the blog of digital rights lobby group the Electronic Frontier Foundation, Peter Eckersley, said the attack posed a "dire risk to internet security".

"The incident got close to — but was not quite — an internet-wide security meltdown," he said.

"We urgently need to start reinforcing the system that is currently used to authenticate and identify secure websites and e-mail systems," said Mr Eckersley.

4 September 2011 Last updated at 09:00 GMT

Iran's Bushehr nuclear plant connected to national grid

The reactor's generating unit at Bushehr began operating at a low level in May

Iran's first nuclear power station has been connected to the country's electricity grid, state news reports.

Bushehr was supplying 60 megawatts of its 1,000 megawatt capacity to the national grid, officials said.

The reactor's generating unit began operating at a low level in May, prompting Israel and other nations to express fears the reactor could help Iran develop nuclear weapons.

Tehran says its intentions are purely peaceful.

But the International Atomic Energy Agency (IAEA) has said it is "increasingly concerned" that Iran is also secretly working on components for a nuclear weapons programme.

Dogged by delays

Iran's Atomic Energy Organisation said the plant in the country's south was connected to the national grid at 23:30 (19:00 GMT) on Saturday.

The connection had initially been scheduled for late last year but, as with developments at Bushehr since the project began in the 1970s, it was dogged by delays.

Construction on the plant was abandoned after Iran's 1979 Islamic revolution until the mid-1990s, when Moscow reached a billion-dollar deal with Tehran to complete it.

In February, Iran had to remove fuel from the reactor "for technical reasons", amid speculation that the Stuxnet computer virus may have been responsible.

The United States and other Western nations for years urged Russia to abandon the project, warning it could help Iran build atomic weapons.

But an agreement obliging Tehran to repatriate spent nuclear fuel to Russia eased those concerns.

In February, an IAEA report obtained by the BBC and made available online by the Institute for Science and International Security (Isis) - said Iran was "not implementing a number of its

obligations."

These included "clarification of the remaining outstanding issues which give rise to concerns about possible military dimensions to its nuclear programme".

Six world powers are negotiating with Iran over its nuclear programme, and the country is subject to United Nations Security Council sanctions over its refusal to halt uranium enrichment.

Enriched uranium can be used for civilian nuclear purposes, but also to build atomic bombs.