http://www.thenational.ae/news/world/middle-east/iran-likely-to-seek-revenge-by-stealth-for-cyber-attacks-expert

Iran likely to seek revenge 'by stealth' for cyber-attacks: expert

Michael Theodoulou

Nov 7, 2012

When Iran's nuclear programme came under an unprecedented cyber-attack and its economy was battered by sanctions, observers doubted Tehran would sit back passively and soak up the punishment.

But how would Iran hit back? Any measures were likely to be stealthy, deniable and calibrated to avoid heavy retaliation from the United States.

In June, Gary Sick, an Iran expert who served on the US National Security Council under presidents Gerald Ford, Jimmy Carter and Ronald Reagan, said Iranian payback might take the form of cyber-attacks on Gulf Arab oil production facilities that could send global energy prices soaring.

After all, the US and Israel were believed to have drawn first blood more than two years ago with an electronic assault on Iran's uranium enrichment programme. Iran also says its oil facilities have come under repeated cyber-strikes this year.

Mr Sick warned that the US, with so much of its infrastructure linked to the internet, was potentially more vulnerable to cyber-attack than any other country.

"If your local power grid goes down, or if your sewage plant blows up… will your first thought be: oh it's those Iranians up to no good?" he wrote in his blog. "Perhaps that possibility should cross your mind."

It has certainly crossed the mind of policymakers in Washington. The US, however, has held back from publicly blaming Iran for a recent spate of cyber-attacks on US banks and on the energy infrastructure of two of its key Gulf Arab allies, Saudi Arabia and Qatar.

Earlier this month the US defence secretary, Leon Panetta, warned that the US was at risk of a "cyber-Pearl Harbour". Washington, he said, is finalising rules of engagement for this uncharted new form of warfare.

Mr Panetta revealed that a wave of network attacks in August crippled 30,000 computers at Saudi Arabia's state-owned Aramco, the world's largest oil company. Data was erased and replaced by a photo of a burning US flag, but oil production was not disrupted.

The same 'Shamoon' virus hit Qatar's RasGas company, a joint venture between the US's Exxon Mobil and the emirate's state-owned Qatar Petroleum, which operates the world's largest natural gas field.

Mr Panetta also said some large US financial institutions were recently hit by attacks that disrupted services on customer websites, although these did not involve any theft of money.

He did not directly accuse Iran of responsibility for any of these attacks, but said Tehran had "undertaken a concerted effort to use cyberspace to its advantage".

Leading US media, however, swiftly cited unnamed US intelligence officials saying they were convinced Iran was behind the various attacks.

Computer viruses have long been used for spying or by organised crime. But the first-known use of a cyber-weapon designed to sabotage an element of another country's infrastructure was the Stuxnet virus -- widely believed to have been jointly developed by the US and Israel.

The virus, discovered in June 2010, attacked Iran's uranium enrichment programme. It was seen as a way to slow Iran's nuclear programme without resorting to military action.

But Stuxnet set a dangerous precedent, establishing that digital warfare could be used in peacetime for essentially political and national security purposes. The US and Israel are now worried about being targeted themselves.

Moreover, experts say any victim of a cyber-attack, such as Iran, can swiftly reverse-engineer the weapon it is hit by and use it to bolster its own digital arsenal.

"Each new cyber-attack becomes a template for other nations - or sub-national actors - looking for ideas," R Scott Kemp, an assistant professor of nuclear science, warned in an October *Bulletin of the Atomic Scientists*, a Chicago-based online magazine.

"A Stuxnet-like attack," he added, "can now be replicated by merely competent programmers, instead of requiring innovative hacker elites."

So, sophisticated cyber weapons, painstakingly developed by technologically advanced nations, could become weapons of the weak.

Page 2 of 2

Sceptics argue that evidence linking Iran to the spate of recent cyber-attacks is largely circumstantial and that most media reports used anonymous sources.

The New York Times acknowledged "there is no hard evidence" the attacks were sanctioned by the Iranian government. And the *Washington Pos*t reported that some security experts outside the US government believed Iran was not behind the Shamoon virus.

The group that claimed responsibility for the electronic attacks on US financial institutions - the so-called Al-Qassem Cyber Fighters - denied it had any connection to Iran, saying its aim was to protest against an anti-Islam video made in California.

Certainly, Tehran has ample motive for all such attacks, including the desire to hit back against western sanctions and to punish Saudi Arabia for bolstering oil supplies to customers no longer buying embargoed Iranian oil. Iran also has an interest in demonstrating it has the means to retaliate in kind against cyber-attacks by its enemies.

But Tehran has vehemently denied all involvement in any cyber-attacks. It insists western accusations are a "smokescreen" to "demonise" Tehran while the US and Israel press ahead with cyber strikes against Iran that, until now, has been the main victim of digital warfare.

Proving definitively who was behind a cyber-strike is very difficult because identities can easily be disguised.

Hence the attraction of cyber-warfare to a country like Iran which is reluctant to take conventional retaliatory action – such as closing the Strait of Hormuz – that could trigger a withering US military backlash.

"The US would need really solid evidence pointing to Iran to justify to the international community [military] retaliation for a cyber-attack," said Dina Esfandiary, an Iran specialist at London's International Institute for Strategic Studies. "One of the primary benefits of cyber-attacks ... is that it's really hard to trace back to the person that's launched the attack."

After the Stuxnet attack, Ms Esfandiary added, Iran created a "cyber army" under the aegis of its Revolutionary Guards. Money was poured into developing digital defences to draw reach cyber parity with the US and Israel.

In what was seen as a veiled threat against Iran, Mr Panetta said the US military "has developed the capability to conduct effective operations to counter [cyber] threats to our national interests".

But, apart from bolstering cyber-defences, what form could such operations take? And what constitutes an act of war in cyberspace that could justify a military response? In September the US State Department's chief legal adviser, Harold Koh, defined an armed attack in cyberspace as one that results in death, injury or significant destruction, comparable to the damage a bomb or missile would inflict.

But proving who launched a cyber-strike could prove the biggest hurdle. Little wonder, then, that Mr Panetta said the Pentagon is investing heavily in forensics to "identify attackers".

When Iran's nuclear programme came under an unprecedented cyber-attack and its economy was battered by sanctions, observers doubted Tehran would sit back passively and soak up the punishment.

But how would Iran hit back? Any measures were likely to be stealthy, deniable and calibrated to avoid heavy retaliation from the United States.

In June, Gary Sick, an Iran expert who served on the US National Security Council under presidents Gerald Ford, Jimmy Carter and Ronald Reagan, said Iranian payback might take the form of cyber-attacks on Gulf Arab oil production facilities that could send global energy prices soaring.

After all, the US and Israel were believed to have drawn first blood more than two years ago with an electronic assault on Iran's uranium enrichment programme. Iran also says its oil facilities have come under repeated cyber-strikes this year.

Mr Sick warned that the US, with so much of its infrastructure linked to the internet, was potentially more vulnerable to cyber-attack than any other country.

"If your local power grid goes down, or if your sewage plant blows up… will your first thought be: oh it's those Iranians up to no good?" he wrote in his blog. "Perhaps that possibility should cross your mind."

It has certainly crossed the mind of policymakers in Washington. The US, however, has held back from publicly blaming Iran for a recent spate of cyber-attacks on US banks and on the energy infrastructure of two of its key Gulf Arab allies, Saudi Arabia and Qatar.

Earlier this month the US defence secretary, Leon Panetta, warned that the US was at risk of a "cyber-Pearl Harbour". Washington, he said, is finalising rules of engagement for this uncharted new form of warfare.

Mr Panetta revealed that a wave of network attacks in August crippled 30,000 computers at Saudi Arabia's state-owned Aramco, the world's largest oil company. Data was erased and replaced by a photo of a burning US flag, but oil production was not disrupted.

The same 'Shamoon' virus hit Qatar's RasGas company, a joint venture between the US's Exxon Mobil and the emirate's state-owned Qatar Petroleum, which operates the world's largest natural gas field.

Mr Panetta also said some large US financial institutions were recently hit by attacks that disrupted services on customer websites, although these did not involve any theft of money.

He did not directly accuse Iran of responsibility for any of these attacks, but said Tehran had "undertaken a concerted effort to use cyberspace to its advantage".

Leading US media, however, swiftly cited unnamed US intelligence officials saying they were convinced Iran was behind the various attacks.

Computer viruses have long been used for spying or by organised crime. But the first-known use of a cyber-weapon designed to sabotage an element of another country's infrastructure was the Stuxnet virus -- widely believed to have been jointly developed by the US and Israel.

The virus, discovered in June 2010, attacked Iran's uranium enrichment programme. It was seen as a way to slow Iran's nuclear programme without resorting to military action.

But Stuxnet set a dangerous precedent, establishing that digital warfare could be used in peacetime for essentially political and national security purposes. The US and Israel are now worried about being targeted themselves.

Moreover, experts say any victim of a cyber-attack, such as Iran, can swiftly reverse-engineer the weapon it is hit by and use it to bolster its own digital arsenal.

"Each new cyber-attack becomes a template for other nations - or sub-national actors - looking for ideas," R Scott Kemp, an assistant professor of nuclear science, warned in an October *Bulletin of the Atomic Scientists*, a Chicago-based online magazine.

"A Stuxnet-like attack," he added, "can now be replicated by merely competent programmers, instead of requiring innovative hacker elites."

So, sophisticated cyber weapons, painstakingly developed by technologically advanced nations, could become weapons of the weak.

Sceptics argue that evidence linking Iran to the spate of recent cyber-attacks is largely circumstantial and that most media reports used anonymous sources.

The New York Times acknowledged "there is no hard evidence" the attacks were sanctioned by the Iranian government. And the *Washington Pos*t reported that some security experts outside the US government believed Iran was not behind the Shamoon virus.

The group that claimed responsibility for the electronic attacks on US financial institutions - the so-called Al-Qassem Cyber Fighters - denied it had any connection to Iran, saying its aim was to protest against an anti-Islam video made in California.

Certainly, Tehran has ample motive for all such attacks, including the desire to hit back against western sanctions and to punish Saudi Arabia for bolstering oil supplies to customers no longer buying embargoed Iranian oil. Iran also has an interest in demonstrating it has the means to retaliate in kind against cyber-attacks by its enemies.

But Tehran has vehemently denied all involvement in any cyber-attacks. It insists western accusations are a "smokescreen" to "demonise" Tehran while the US and Israel press ahead with cyber strikes against Iran that, until now, has been the main victim of digital warfare.

Proving definitively who was behind a cyber-strike is very difficult because identities can easily be disguised.

Hence the attraction of cyber-warfare to a country like Iran which is reluctant to take conventional retaliatory action – such as closing the Strait of Hormuz – that could trigger a withering US military backlash.

"The US would need really solid evidence pointing to Iran to justify to the international community [military] retaliation for a cyber-attack," said Dina Esfandiary, an Iran specialist at London's International Institute for Strategic Studies. "One of the primary benefits of cyber-attacks ... is that it's really hard to trace back to the person that's launched the attack."

After the Stuxnet attack, Ms Esfandiary added, Iran created a "cyber army" under the aegis of its Revolutionary Guards. Money was poured into developing digital defences to draw reach cyber parity with the US and Israel.

In what was seen as a veiled threat against Iran, Mr Panetta said the US military "has developed the capability to conduct effective operations to counter [cyber] threats to our national interests".

But, apart from bolstering cyber-defences, what form could such operations take? And what constitutes an act of war in cyberspace that could justify a military response? In September the US State Department's chief legal adviser, Harold Koh, defined an armed attack in cyberspace as one that results in death, injury or significant destruction, comparable to the damage a bomb or missile would inflict.

But proving who launched a cyber-strike could prove the biggest hurdle. Little wonder, then, that Mr Panetta said the Pentagon is investing heavily in forensics to "identify attackers".