Intelligence brief | 18 November 2013

Iran's cyber posture

In early October 2013, the death of a hitherto little known individual by the name of Mojtaba Ahmadi was reported near Karaj, slightly northwest of Tehran. Ahmadi was shot twice in the chest from a passing motorcycle according to an eyewitness account in the Iranian press that was later taken offline. A statement by the Iranian Revolutionary Guards Corps (IRGC) in contrast denied that an assassination had taken place, adding only that investigations were underway. As it turned out, Ahmadi was a key cyber warfare commander, and possibly Iran's cyber war chief.

The truth of the matter aside, this event brings to mind the spate of Iranian nuclear scientists who were targeted in similar circumstances over the past seven years. In addition to assassination attempts, the covert tit-for-tat war between Iran on the one hand, and the United States, Israel and various Western allies on the other has steadily expanded to include a cocktail of diplomatic pressure, economic sanctions, attacks directed at civilians overseas, and now, a virtual war with real-life consequences. By force of circumstance as much as by design, Iran has responded in kind and is clearly channelling greater resources towards its own cyber front.

Force structure and capabilities

The Iranian authorities have been policing domestic websites, social media and virtual private networks (VPNs), mainly with Chinese assistance, in order to clamp down on dissent and interdict soft influences from abroad, especially after the Green Movement protests of mid-2009. A **Cyber Police** unit (FETA) was set up in 2009 to combat internet crimes and neutralise online dissent networks and enforce Islamic cyberspace decorum (the latter in tandem with the **Committee for the Identification of Unauthorised Websites**, which reports to the Supreme Council of the Cultural Revolution). The Iranian government has also taken steps to implement an alternative search engine (dubbed *Ya Hagh*, 'Oh God' [Truth]) and is planning a parallel, 'halal' Iran-only internet network. It has matched these moves by slowing down regular internet speeds in order to eventually discourage its use.

The idea of cyber defence was purportedly raised with the leadership as far back as 2005 but Iran's cyber policy only effectively took shape in the wake of the Stuxnet attacks discovered in late 2010.

Open Briefing
27 Old Gloucester Street
Bloomsbury
London WC1N 3AX

t 020 7193 9805
info@openbriefing.org
www.openbriefing.org

A **Cyber Defense Command** (*Qarargah-e Defa-e Sayberi*) was established under the jurisdiction of the Passive (or Civil) Defence Organisation (*Sazeman-e Padafand-e gheyr-e amel*) and ultimately, the Joint Staff of the Armed Forces. Headed by Brigadier-General Gholam-Reza Jalali, the Passive Defence Organisation has also over recent years overseen a large number of country-wide cyber readiness drills. In March 2012, upon its initiative, cyber defence programmes went online in a number of Iranian universities. Also in March 2012, the **Supreme Council of Cyberspace** (*Shora-ye Ali-ye Faza-ye Majazi*), which subsumes all other cyber organisations under its fold, came into being by decree of the Supreme Leader. This was a clear signal that cyber warfare was henceforth to be regarded as a strategic threat, and cyberspace a distinct arena for Iran's ongoing conflict with Western status quo powers and Israel.

The series of viruses including Stuxnet, Duqu, Flame and possibly Stars, which attacked its uranium centrifuge programme before targeting other critical sectors, is very likely to have impelled the Iranian government to cross the cyber defense threshold to one of offensive deterrence. Tehran is estimated to have invested over $1 billion in developing an off-the-books **Cyber Army** consisting of a nebulous and highly compartmentaliaed nexus of official and semi-official hacktivists, all of which comes under the command of the IRGC according to the Supreme Leader's representative to the organisation, Ali Saeedi.

A number of other foot soldier-type cyber battalions have come online within the paramilitary Basij volunteer force, organised around the **Basij Cyberspace Council.** According to reports, members of the latter engage in massive pro-regime public diplomacy campaigns as well as the tracking and removal of anti-regime content. Furthermore, independent, competing groups such as Ashiyane, Jehad-e Gomnam-e Majazi (Virtual Anonymous Jihad), Shabgard and Simorgh are known to have authored highly visible hacking campaigns in increasing cooperation with the Iranian government. Lastly, in addition to cyber units affiliated with Hezbollah, Syria, and allegedly to some extent, Hamas, Iran may conceivably be enlisting the assistance of other actors, both state and non-state, far beyond its borders.

In July 2011, a spyware traced back to Iran and dubbed Mahdi, with capabilities not dissimilar from those of Flame, was discovered infecting infrastructural targets in Israel and a number of states around the Persian Gulf. But rather than pure espionage, the trend has shifted towards cyber offensives. In August 2012, a group known as the Cutting Sword of Justice unleashed a virus dubbed Shamoon on the internal communications network belonging to Saudi Arabia's Aramco state oil corporation. The virus blanket-deleted crucial data in three-quarters (i.e. 30,000) of the company's computers and replaced it with the image of a burning US flag. Another attack took place a fortnight later against RasGas, Qatar's key liquefied natural gas producing company. Between September 2012 and January 2013, a group known as the Ezzeddin al-Qassam Cyber Fighters carried out multiple distributed denial-of-service (DDoS) attacks against several major US financial institutions including Bank of America Corp, CitiGroup, JPMorgan, Chase and Wells Fargo. This amounted to attacks against US targets on US territory.

Iranian hackers are also believed to have carried out cyber attacks on a large number of websites belonging to foreign governments (e.g. the United States, the United Kingdom, France, the Persian Gulf states, Israel and China), commercial entities (e.g. Dutch web security firm DigiNotar), media outlets (e.g. Radio Zamaneh and Voice of America Persian) and social networks (e.g. Twitter).

Intentions

Unlike most other states in the Middle East, Iran possesses the human and technological resources to turn cyberspace into a battlefield; according to some sources, it already ranks among the top five cyber states – along with the United States, Russia, China and Israel. The record suggests that Iran's military cyber policy (in contradistinction to domestic surveillance) remains largely defensive in character. But it is increasingly difficult to draw a clear line between offensive and purely defensive means, an exercise that would have been more practicable in the previous century.

Iran's cyber conduct closely mirrors that of its offline security doctrine, which is in the first instance predicated on the defence of its sovereign territory and the Persian Gulf and Strait of Hormuz. A secondary but significant aspect is the deployment and activation of assets beyond its borders in ways that actively deter potential aggressors. Where this fails, retaliation can be expected, which has been the case both offline and online.

Iran's emerging cyber posture fits hand-in-glove within its current palette of strategic responses owing to its asymmetric character (outsized yield for a relatively low input, and against a conventionally superior adversary), the high degree of plausible deniability it confers, the possibility of outsourcing expertise, and more importantly, the active deterrence emplaced against what Tehran perceives, with justification, as attacks initiated against it. Recall that Iran started enhancing its cyber capabilities in earnest following the attacks targeting its centrifuges in the Natanz uranium enrichment facility. Given that the United States and Israel are also prime movers in the cyber domain who seek increasing recourse to it as a weapon of preference, Iran should be expected to respond in kind.

Implications

Cyberspace provides a mediated environment for alternative forms of warfare. While this, *prima facie*, avoids the risks of direct kinetic confrontation, the results can have very tangible and therefore disruptive consequences on the life of a society and the economy that keeps it going. If Stuxnet, which is believed to have been jointly scripted by the United States and Israel, could wreck physical damage on Iran's centrifuges by merely upsetting their spin frequencies, any other critical installation dependent on computerised accuracy and reliability is likewise vulnerable. Given that banking systems, the stock exchange and critical infrastructure such as power, transportation and communications grids in modern-day cities are patched into cyberspace, massive havoc is only a matter of ability and execution.

Contemporary weapons systems are also increasingly hotwired into highly integrated command, control, communications, computers and intelligence networks and are hence exposed to similar vulnerabilities. In more complex wartime scenarios, cyber operations could aim at disrupting critical infrastructure simultaneously or near-simultaneously with actual kinetic offensives.

In addition, there are a number of issues specifically associated with cyber warfare:

- Although imperfect information is a constant in any theatre of operations (the 'fog of war'), a surface-to-surface missile for instance can rather easily be traced back to its origins. The cyberspace medium on the other hand militates against unambiguous attribution of acts of aggression. In the absence of certainty, decision-makers are obliged to shape a response based only on a suboptimal threshold of error. How does one then determine that threshold, and the corresponding yardsticks for decision-making, if there is no smoking gun? IP addresses, for example, have become extremely fluid and manipulable, allowing an infinite regression of false flag operations. An alternative is to match perpetrators against their known cyber capabilities, but even then this may only render one suspect more *probable* than others, not *certain*.
- Because cyberspace by its nature merges the military with the civilian, cyber warfare likewise fails to discriminate between combatants and civilians. This is a distinction enshrined in the Fourth Geneva Convention, which has for the past half-century lain at the basis of the laws regulating armed conflict. Therefore, cyber warfare clearly necessitates a distinct international regulatory framework. Furthermore, it is not always clear, for instance, whether homeland cyber defence should fall within the remit of the military, domestic law enforcement or civilian structures.
- Traditional security concepts, such as deterrence, clearly remain valid but require fundamental rethinking in cyberspace where borders melt away and the topography of warfare has been altered.
- Cyber connectivity renders entire societies more vulnerable and exposed than ever. When coupled with the problem of attribution, this requires an extremely robust defensive posture first and foremost.
- As it stands, the key advantage that inheres within a cyber attack is its plausible deniability. Assuming this consideration to be preponderant, a battleplan entailing a simultaneous (or near simultaneous) kinetic offensive will need to be designed differently. The question also follows if a cyber offensive can elicit a strictly cyber response, without recourse to conventional kinetic means.

Projections

Given the increased stakes and the asymmetric advantages associated with cyberspace, Iran is **highly likely** to ramp up its online capabilities and activities, especially for so long as the standoff with Western powers and Israel continues. However, given its defence posture, Iran is also **highly likely** to refrain from full-scale cyber offensives, barring retaliation to what it deems to be acts of war.

Open Briefing is the world's first intelligence agency for civil society. We produce actionable and predictive intelligence. We tell you what has happened and what is likely to happen next. Most importantly, we tell you why.

We do this so that better informed citizens can more effectively engage in peace and security debates and civil society organisations can make the right advocacy choices. Together, we can then influence positive defence, security and foreign policy decisions by our governments.

Open Briefing is an innovative and dynamic not-for-profit social enterprise. We are a unique international collaboration of intelligence, military, law enforcement, government and media professionals.

www.openbriefing.org