NATO Foundation
Defense College

Emerging Challenges October 2017

Iran's Threat is more Cyber than Nuclear

On 19 September 2017, US President Trump made a vibrant attack at the UN on Iran, criticising its nuclear programme and its unspecified support of Islamic terrorism. On 13 October, the President reiterated his accusations on Teheran. Trump announced that he would terminate the 2015 Iran nuclear deal if the US Congress and US allies fail to make it more severe. In his view, Obama's deal – "an embarrassment to the US" – is insufficient to contain Iran's menace. However, even if Teheran did decide to pursue its nuclear programme in violation of the deal – which has never been proved – it is unlikely that its nuclear facilities can pose a real danger in the near future. Iran's more immediate threat falls in a different domain – namely cyber space.

Iran's rapid development of its cyber-capabilities was stimulated by the 2010 Stuxnet attack – a successful Israeli and US-led sabotage of Iran's nuclear program. Ever since, the US Army's Strategic Studies Institute has chronicled the rise of Iranian cyber forces. In 2011, Teheran invested $1 billion in cyber technology, infrastructure, and expertise. In 2012, the élite Iranian Revolutionary Guard Corps (IRPG) announced that it had recruited a remarkable 120,000 cyber personnel. Recently, Rouhani has increased the IRPG annual cybersecurity budget to $19.8 million, encouraging the training of 1,500 private cyber-warriors. According to Ian Bremmer, president of the global consulting firm Eurasia Group, Iran's cyber capabilities are expanding faster than anyone "would have ever imagined" and could soon prove "more troubling than its nuclear programme." True, Iran falls behind America and its strongest cyber adversaries, China and Russia. But this is precisely reason why it represents a unique and in some ways more troubling threat.

First, Iranian attacks appear less restrained and more intent on causing harm to US institutions, rather than merely targeting in cyber espionage. Iran has been linked to attacks against billionaire casinos in Las Vegas and numerous US banks, including the Bank of America, Citigroup, Wells Fargo, and HSBC, and to Twitter hacks of US press groups, including CNN, Time and The Washington Post. Such targets have no strategic value, but are well-known to the public – thus allowing Iran to gain maximum propaganda.

Second, whilst Iran is still behind the world's superpowers, its cyber capabilities are considered to be on an equal footing with Israel's and superior to those of the other regional powers in the Middle East. Iran can target its neighbouring rivals in a number of ways, such as disrupting their news organisations, financial systems, energy infrastructures and military or law enforcement communication – as demonstrated by Iran's attack on Saudi Aramco, Riyadh's national petroleum and natural gas company. Thus, Teheran's cyber capabilities can re-shape the geopolitical balance in the region.

Third, Iran's new private cyber-warriors can allow Teheran to empower its proxies with cyber-capabilities. Iran has long been a supporter of terrorist organisations in Lebanon, Yemen, and Syria, and is likely to have contributed to the creation of the Syrian Electronic Army in support of Assad, and the Yemen Cyber Army in support of the Houthis against the Yemenite government and Saudi Arabia. Private actors are more difficult to combat because they raise serious problems of attribution. Furthermore, Iran may not have – or may lose – direct control over its cyber-proxies, with unpredictable consequences.

In contrast to the Iranian nuclear programme, Iran's cyber-forces draw much less attention and cannot be monitored as easily as a nuclear programme. Yet they have the capacity to lead to local cyber-confrontations, which can easily turn into conventional war, and therefore represent a serious threat in the region and beyond.

Stefano Marcuzzi - *PhD in Military History at the University of Oxford, he is now a Max Weber Fellow at the EUI Florence, working on hybrid warfare and EU-NATO relations in the Mediterranean*