Iran: Prospective, Rapid Technological Breakthroughs

Jeremy Vaughan

IISS The International Institute for Strategic Studies

www.iiss.org

Iran: Prospective, Rapid Technological Breakthroughs

An Iranian animated film released in February 2017 depicts Iran using sophisticated technology to win an asymmetric battle against the United States.[1] In the film, Iran's military uses surface-to-surface missiles, remote-controlled mini-tanks and ballistic missiles to destroy US Navy ships and special forces. In reality, Iran has developed rudimentary versions of these weapons, including a relatively accurate replication of the movie's remote-controlled tank, and provided them to its proxies in the greater Middle East.[2]

Citing US sanctions (enacted prior to the signing of the Joint Comprehensive Plan of Action or JCPOA), Apple banned Iranian apps from its App Store in August 2017, causing large disruption to the nation's burgeoning technology start-up culture.[3] However, as Iran continues its current path of normalization with the international community, it will increasingly have access to new civilian technologies. Moreover, once the arms restrictions specified in the UN Security Council Resolution 2231 ease in 2020, Iran will be able to purchase advanced military technology. Without targeted sanctions or other alternative measures, advances in autonomy and artificial intelligence (AI) will eventually provide Iran and its proxies with new ways to quickly advance their military capabilities, potentially reshaping the region without tripping traditional counter-proliferation alarms.

Technology as a weapon

The neutralization of an adversary's superior military force through the use of technology is not a new strategy for either the United States or Iran. During the early years of the Cold War, the US offset the Soviet Union's formidable conventional force, first by developing small-yield battlefield tactical nuclear weapons, and then precision-guided munitions. Ballooning weapons costs, budget constraints and emerging peer adversaries are driving the United States to pursue the latest 'third offset' strategy by developing and exploiting AI and autonomous systems.[4]

Along somewhat similar lines, Iran's heavy investment in cyber technology in the 2000s highlights the country's early-adopter mindset, and offers insight into how it might exploit technology to gain an advantage in the future. While Iranian cyber activity was initially limited to website defacement, it became much more advanced after the 2007 Stuxnet attack infected its uranium-enrichment infrastructure.[5] Following its successful and sophisticated attacks on American and Saudi Arabian infrastructure, Iran – along with North Korea – is often considered to possess capabilities just below those of the United States, Russia, China and Israel.[6]

Autonomy is coming to Iran

Large commercial investments in unmanned autonomous systems – those 'that can change their behavior in response to unanticipated events' – have significantly increased in recent years, and such systems are quickly growing in capability.[7] Companies like Amazon and Google are pushing the boundaries of adaptable

guidance through the development of self-driving cars and autonomous-drone package delivery. In 2016, Waymo – spun off from Google's self-driving car project by parent company Alphabet – drove autonomously for over 2.3 million miles, and Amazon's drone service delivered its first packages in the UK.[8] It's not just corporations that are using this technology: an American software engineer built a surprisingly capable self-driving car in his garage by incorporating computer and sensing systems with an algorithm.[9] Iran already possesses a diverse ecosystem of locally produced unmanned aerial vehicles, and the engineering techniques necessary to develop autonomous systems are not beyond Iranian capabilities. Updating Iranian systems to operate autonomously could be as simple as cobbling together additional hardware, and installing acquired algorithms. By doing so, Iran could engineer package drones – like those developed by Amazon – autonomously guided to deliver explosives to designated targets. Such a development could prove to be the precision-guided munitions windfall that has so far eluded Iran and its proxies.

Swarming – a tactic that seeks to overwhelm an adversary through sheer numbers and that is used heavily in Iranian naval doctrine – could also be automated. Such a capability would have substantial potential for asymmetric warfare. While current Iranian capabilities rely on piloted boats, autonomous swarming would require mastery of sensing systems, computer networks and sophisticated algorithms to keep a large number of unmanned boats, drones, tanks or robots in coordinated motion. Though smaller drones individually pack less of a punch than manned combat aircraft, a herd of drones operating as one offers an asymmetric means for targeting an adversary's critical assets or capabilities. A single drone can cause significant disruption through a kamikaze attack on a sensitive target. With the addition of explosives or other payloads, a relatively small swarm of drones could offset a large US conventional military advantage by destroying fragile air- and missile-defense radars, overwhelming point defenses or simply saturating sensing systems.[10] Rapid advances in the group control of drones and swarming techniques, together with cyber capabilities and Iran's burgeoning relationship with China – which involves significant transfer of technology to Iran – could pave the way for Iranian combat capabilities in beyond-line-of-sight drone systems, swarming control and multi-domain (air, surface and underwater) unmanned systems.[11]

Artificial intelligence expands cyber reach

Artificial intelligence – the simulation of intelligent, human behavior in computers – uses very large amounts of data, specialized processing chips and heavily engineered algorithms to change and inform how computers solve complex problems. Computing power and techniques have developed from the earlier use of brute-force processes, to more human-like processes, wherein the system is exposed to a large database of information and uses algorithms and neural networks to improve its decision-making.[12] Apple's newly released iPhone X provides an example of the latter's use in a commercial context. The beating heart of this device is its AI chip, which enables facial recognition of the user to unlock the phone – an industry first – and can make over 600 billion calculations per second. The fact that these capabilities are included in a cellphone developed by the private sector, rather than the US military, should give operational and tactical planners pause for thought, to reflect on how adversaries such as Iran could adapt or acquire such technologies.[13] State actors are already using analogous cyber capabilities to probe and shore up defensive gaps, and to find new ways to access target systems. Gaining access to advanced AI algorithms through theft or open-source codes could provide Iran with cyber capabilities that could further unbalance the region.

Can Iran achieve advanced technological breakthroughs?

Despite Iran's rising military budgets, recognized scientific talent and asymmetric mindset, skeptics argue that rapid technological breakthroughs are beyond its capability.[14] At first glance, such doubts appear justified, given that Iran includes among its advertised maritime-weapons forces jet-skiers wielding rocket-propelled grenades.[15]

Operational problems will likely not prove too difficult for Iran to surmount. Iran has continued an old Persian tradition of emphasizing mathematics and science in education. Iranian students finish well in mathematics competitions – its team finished fifth in the 2017 International Mathematics Olympiad, behind South Korea, China, Vietnam and the United States. The best Iranian mathematician in the competition tied for first in the world. In the last decade, Iran has finished tenth or better six times, winning 14 individual gold medals.[16] While many of the country's brightest minds have historically left Iran, years of sanctions are slowing this brain drain by restricting access to foreign schools and feeding them back into Iran's highly subsidized engineering fields.[17]

While some argue that the arms embargo has successfully stopped Iran's technological advancement, Iran has found ways to improve its capabilities despite the sanctions.[18] While Iran lacks the industrial infrastructure to produce advanced fighter aircraft, it has been an innovator in the development and use of unmanned aircraft since the 1980s.[19] Despite international embargoes, export laws and treaties restricting Iran's access to light turbofan and turbojet engines, and other key aviation components, Iranian drone technicians have continued to acquire the necessary parts – either through local manufacture or on the black market.[20] While it is true that no drone can match American airpower, asymmetric tactics and the deployment of technologies like swarming, miniature submarines, mines and salvos of anti-ship cruise missiles would be a significant challenge for any military force.[21] Marginal improvements in autonomous drone control alone could significantly raise the cost of future combat for Iran's adversaries. More importantly, Iranian technological improvements tend to immediately trickle down for use in proxy warfare. In the last decade alone, Iranian proxies have critically damaged an Israeli patrol boat and nearly sunk an Emirati warship, using anti-ship cruise missiles in both cases. Elsewhere, a remote-controlled tank has been deployed in battle by the Iranian-backed Iraqi Popular Mobilization Units against the Islamic State, also known as ISIS or ISIL. In Yemen, Houthi rebels successfully guided a small, unmanned boat laden with explosives – likely an Iranian innovation – into a Saudi Arabian frigate. Although Saudi Arabia and other Gulf countries outspend Iran on defense by a ratio of more than five to one, advances in artificial intelligence and autonomy could eventually offset this disparity and destabilize the region.

Planning for the future

Iran will undoubtedly continue to improve its asymmetric military capabilities through leveraging technology. However, the risk of technological breakthroughs can be mitigated if the US, its allies and partners, and the wider international community take immediate and decisive action.

Existing non-proliferation tools like the Missile Technology Control Regime (MTCR) are not likely to impede Iran's efforts to develop the algorithms which will enable autonomous swarming and other tactics. The MTCR will, however, make it more difficult for Iran to access small, efficient propulsion systems for its drones. Executive orders by the US that sanctions against those who carry out technology transfers to Iran have greater efficacy than multilateral control mechanisms. The US Treasury's Office of Foreign Assets Control's (OFAC) designation of 16 entities in 2017 for technological support to Iran shows that such action is possible.[22] The creation of a 'Countering Technology Threat' (CTT) program, based on extant and effective Countering Terrorist Financing (CTF) programs, would use these same mechanisms while providing more focus on the illegal transfer of technology. CTF programs are powerful, because financial transactions denominated in US dollars must go through American exchanges and are therefore subject to American law. Similarly, as many of the technological advances are being made in the United States, a CTT program could greatly expand the use of US export laws focused on restricting and prosecuting illegal software proliferation, protecting the homeland and American businesses.

Despite concern about the risks of artificial intelligence by field leaders like Tesla and SpaceX CEO Elon Musk, advanced AI code is freely available for use and is circulated globally.[23] Iran has proved willing to steal technology it cannot access for free, permitted by the often

porous information systems used in the commercial sector.[24] Corporations could secure their systems, maximize their research potential and perhaps gain some say in how new technologies are used in warfare, through integrating their AI development with that of the US government in joint public-private ventures.[25] Intel's collaboration with the Defense Advanced Research Projects Agency (DARPA) on the Hierarchal Identity Verify and Exploit (HIVE) AI system shows how fruitful such partnerships can be.[26]

Hardware alignment in unmanned systems must be tracked to adequately warn military planners before new capability leaps mature. Much as an old flip-front cellphone cannot become the latest iPhone by just downloading new software, sudden capability shifts cannot happen by stealing new operating-system code. Similarly, an Android mobile device cannot be updated through an Apple software download, because the operating systems are so different. However, if hardware and software are aligned, greatly improved capability could be just a download away. DJI, the world leader in consumer unmanned aerial vehicles, required all owners to download software that prohibited their devices flying in certain areas, after the company received withering criticism following use of their products by extremists.[27] While these downloads restricted capability, the opposite is also possible. Drone hardware aligned sufficiently with third-party control software could potentially transform an airspace hazard into a swarming nightmare overnight.

The US and its allies must plan now to meet a more advanced adversary, before a technological leap in Iran's capabilities occurs. The military-acquisition system must begin to develop weapons able to counter emerging technologies. For AI, the development of cyber techniques to corrupt databases necessary for machine learning could neutralize a system before it can be used.[28] In order to combat autonomous weapons systems, directed-energy weapons could disable swarming threats without depleting conventional ammunition. In all cases, military lawyers must determine how the laws of armed conflict will apply to new technologies and produce rules of engagement that will enable military commanders to defeat robotic systems.[29]

Superpowers will not enjoy monopolies on any future technological leaps, and the advantages afforded by any such leaps might prove short-lived. The trickle down of advanced capability, however diluted, means that they will in some form eventually be used by Iranian proxies, which will increase the cost of intervention and change the regional balance of power. If the US and its international partners take action now to more carefully monitor the development of Iran's military systems, and to slow the transfer of technology to the country, they can forestall the unwelcome scenario of dramatic improvements to its capabilities.

Cmdr Jeremy Vaughan, US Navy, is a former Federal Executive Fellow at The Washington Institute who has completed multiple deployments to the Persian Gulf. The views expressed herein are those of the author and do not reflect the official policy or position of the US Navy, US Department of Defense, or US government.

Notes

1 Hope Hodge Seck, 'New Animated Film Depicts Iran Defeating US Navy', Defense Tech, 22 February 2017, https://www.defensetech.org/2017/02/22/iran-defeats-us-navy-animated-film.

2 Martin Kiser, 'Iraqi PMU Unmanned Ground Vehicle', Armament Research Services, 14 September 2016, http://armamentresearch.com/iraqi-pmu-unmanned-ground-vehicle.

3 'AI Untethered: Where to Draw the Line on Artificial Intelligence?', France24, 8 September 2017, http://www.france24.com/en/20170908-tech24-ai-artificial-intelligence-iran-apps-apple-embargo-star-wars-gadgets.

4 Bob Work, 'Deputy Secretary of Defense Speech: The Third U.S. Offset Strategy and Its Implications for Partners and Allies', US Department of Defense, 28 January 2015, https://www.defense.gov/News/Speeches/Speech-View/

Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies.

5 Kim Zetter, 'The NSA Acknowledges What We All Feared: Iran Learns from US Cyberattacks', Wired, 10 February 2015, https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks.

6 Keith Breene, 'Who Are the Cyberwar Superpowers?', World Economic Forum, 4 May 2016, https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers.

7 D.P. Watson and D.H. Scheidt, 'Autonomous Systems', *Johns Hopkins APL Technical Digest*, vol. 26, no. 4, 2005, pp. 368–76 (p. 368), http://www.jhuapl.edu/techdigest/TD/td2604/Watson.pdf.

8 Waymo, 'Disengagement Report: Report on Autonomous Mode Disengagements for Waymo Self-Driving Vehicles in California', 5 January 2017, available at https://www.dmv.ca.gov/portal/wcm/connect/946b3502-c959-4e3b-b119-91319c27788f/GoogleAutoWaymo_disengage_report_2016.pdf?MOD=AJPERES; Alex Hern, 'Amazon Claims First Successful Prime Air Drone Delivery', *Guardian*, 14 December 2016, https://www.theguardian.com/technology/2016/dec/14/amazon-claims-first-successful-prime-air-drone-delivery.

9 Ashlee Vance, 'The First Person to Hack the iPhone Built a Self-Driving Car. In His Garage', Bloomberg, 16 December 2015, https://www.bloomberg.com/features/2015-george-hotz-self-driving-car.

10 Jeremy Vaughan, 'Foreign Drones Complicate Maritime Air Defense', *US Naval Institute Proceedings*, April 2017, pp. 54–59.

11 Farzin Nadimi, 'Iran and China Are Strengthening Their Military Ties', Breaking Energy, 24 November 2016, http://breakingenergy.com/2016/11/24/iran-and-china-are-strengthening-their-military-ties.

12 Danielle Muoio, 'Why Go Is So Much Harder for AI to Beat than Chess', Business Insider, 10 March 2016, http://www.businessinsider.com/why-google-ai-game-go-is-harder-than-chess-2016-3.

13 James Vincent, 'The iPhone X's New Neural Engine Exemplifies Apple's Approach to AI', The Verge, 13 September 2017, https://www.theverge.com/2017/9/13/16300464/apple-iphone-x-ai-neural-engine.

14 Robert Beckhusen, 'Stop Freaking Out – Iran's Military Is Weak Even Without Sanctions', War Is Boring, 14 July 2015, https://medium.com/war-is-boring/stop-freaking-out-iran-s-military-is-weak-even-without-sanctions-16e84e738c06.

15 Richard Scott, 'Surviving the Swarm: Navies Eye New Counters to the FIAC Threat', Jane's Navy International, March 2014, http://www.janes360.com/images/assets/571/36571/Surviving_the_swarm_new.pdf.

16 International Mathematical Olympiad, '58th IMO 2017: Country Results', https://www.imo-official.org/year_country_r.aspx?year=2017&column=total&order=desc.

17 Julian Taub, 'Science and Sanctions: Nanotechnology in Iran', Scientific American, 13 January 2012, https://blogs.scientificamerican.com/guest-blog/science-and-sanctions-nanotechnology-in-iran; Steven Ditto, Red Tape, Iron Nerve: The Iranian Quest for U.S. Education', Policy Focus 133 (Washington DC: Washington Institute of Near East Policy, 2014), available at https://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus_133_Ditto3.pdf.

18 Trita Parsi and Tyler Cullis, 'The Myth of the Iranian Military Giant', Foreign Policy, 10 July 2015, http://foreignpolicy.com/2015/07/10/the-myth-of-the-iranian-military-giant.

19 Arthur Holland Michael, 'Iran's Many Drones', Center for the Study of the Drone at Bard College, 25 November 2013, http://dronecenter.bard.edu/irans-drones.

20 Adam Rawnsley, 'Like It or Not, Iran Is a Drone Power', War Is Boring, 5 September 2014, https://warisboring.com/like-it-or-not-iran-is-a-drone-power.

21 Julian Borger, 'US Shoots Down Second Iran-Made Armed Drone over Syria in 12 Days', *Guardian*, 20 June 2017, https://www.theguardian.com/us-news/2017/jun/20/us-iran-drone-shot-down-syria.

22 US Department of the Treasury, 'Treasury Targets Persons Supporting Iranian Military and Iran's Islamic Revolutionary Guard Corps', 18 July 2017, https://www.treasury.gov/press-center/press-releases/Pages/sm0125.aspx.

23 See, for example, the data made freely available by Google DeepMind: https://deepmind.com/research/open-source.

24 US Department of Justice, 'Two Iranian Nationals Charged in Hacking of Vermont Software Company', 17 July 2017, https://www.justice.gov/opa/pr/two-iranian-nationals-charged-hacking-vermont-software-company.

25 Gary Marcus, 'Artificial Intelligence Is Stuck. Here's How to Move It Forward.', *New York Times*, 29 July 2017, https://www.nytimes.com/2017/07/29/opinion/sunday/artificial-intelligence-is-stuck-heres-how-to-move-it-forward.html.

26 'Intel Names to DARPA Project Focused on Machine Learning and Artificial Intelligence', Intel Newsroom, 5 June 2017, https://newsroom.intel.com/news/intel-named-darpa-project-focused-machine-learning-artificial-intelligence.

27 Tim Bradshaw, 'Drone Marker DJI Updates Software to Thwart Terrorist Use', *Financial Times*, 29 April 2017, https://www.ft.com/content/317ab47c-2baa-11e7-bc4b-5528796fe35c.

28 Richard Chirgwin, 'Boffins Bust AI with Corrupted Training Data', The Register, 28 August 2017, https://www.theregister.co.uk/2017/08/28/boffins_bust_ai_with_corrupted_training_data.

29 Jeremy Vaughan, 'Foreign Drones Complicate Maritime Air Defense', *US Naval Institute Proceedings*, vol. 143, no.4, April 2017, p. 370, https://www.usni.org/magazines/proceedings/2017-04/foreign-drones-complicate-maritime-air-defense.

The International Institute for Strategic Studies – UK
Arundel House | 6 Temple Place | London | WC2R 2PG | UK
t. +44 (0) 20 7379 7676 **f.** +44 (0) 20 7836 3108 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies – Americas
2121 K Street, NW | Suite 801 | Washington, DC 20037 | USA
t. +1 202 659 1490 **f.** +1 202 659 1499 **e.** iiss-americas@iiss.org **w.** www.iiss.org

The International Institute for Strategic Studies – Asia
9 Raffles Place | #51-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **f.** +65 6499 0059 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Middle East
14th floor, GBCORP Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain
t. +973 1718 1155 **f.** +973 1710 0155 **e.** iiss-middleeast@iiss.org