Navigating Cybersecurity and Surveillance: Iran's Dual Strategy for National Security

by Nima Khorrami **(/experts/nima-khorrami)**

Mar 29, 2024
Also available in
العربية (/ar/policy-analysis/altaml-m-alamn-alsybrany-walmraqbt-astratyjyt-ayran-almzdwjt-llamn-alqwmy)

ABOUT THE AUTHORS

Nima Khorrami (/experts/nima-khorrami)

Nima Khorrami is a Research Associate at the OSCE Academy in Bishkek and an Associate Researcher at the Arctic Institute in Washington DC. He is currently working on a book on the evolving role of cyberspace and cybersecurity in the context of Iran's strategic culture.

Brief Analysis

While Iranian officials acknowledge the significance of cyber tools and AI for foreign policy, they are acutely aware of the country's financial and scientific limitations.

Discussions and debates surrounding the utilization and significance of cyberspace and artificial intelligence in Iran primarily revolve around two key perspectives **(https://www.wiley.com/en-us/Artificial+Intelligence,+Cybersecurity+and+Cyber+Defence-p-9781119788188)** : viewing them as integral components of national security strategy, and understanding cyber capabilities and AI as essential tools for safeguarding national interests. Within the context of Tehran's extensively publicized forward defense doctrine **(https://www.mei.edu/publications/upgrading-irans-military-doctrine-offensive-forward-defense)** , it is reasonable to expect that Tehran would develop (AI assisted) offensive cyber capabilities, allowing it to infiltrate its adversaries' systems and execute preemptive actions against perceived threats. A critical prerequisite for doing so, in turn, would be to put in place robust surveillance capabilities **(https://www.tietoevry.com/en/blog/2018/12/4-key-capabilities-that-every-successful-cybersecurity-operations-possesses/)** which can alarm the officials of any potential incoming attack. However, available evidence suggests a dire lack of such capabilities not least because Iran's critical infrastructure has been the target of frequent cyberattacks, allegedly originating from Israel.

What's particularly noteworthy is that Tehran's existing surveillance capabilities are at present primarily focused on monitoring ordinary citizens, including political activists and opposition figures. This is evident in a batch of recent leaks, documented by Intel471 **(https://intel471.com/blog/irans-domestic-espionage)** , which shed light on the regime's surveillance tactics and the extent of Iran's security forces involvement in both developing and deploying tailored tools and malicious software to monitor individuals within Iran and abroad. One example is the deployment of Abi **(https://arezooyenatamam.wordpress.com/2019/02/21/%25D8%25A7%25D9%2581%25D8%25B4%25D8%25A7%25DB%258C-%25D9%25BE%25D8%25B1%25D9%2588%25DA%2598%25D9%2587-%25D8%25B1%25D8%25AF%25DB%258C%25D8%25A7%25D8%25A8%25DB%258C-%25D8%25A2%25D8%25A8%25DB%258C-%25D9%2588-%25D9%2588%25DB%258C%25D8%25B1%25D9%2588%25D8%25B3-%25D9%25BE%25DB%258C%25D9%2588%25D9%2586%25D8%25AF-2/)** , a surveillance system that intercepts Bluetooth transmissions to monitor political activists, dissidents, and protestors. Positioned on pickup trucks around university campuses and protest hotspots, Abi represents a pervasive form of surveillance used to suppress dissent and opposition to the regime. Similarly, WinspySuite demonstrates the regime's commitment to extracting sensitive information from its citizens' devices. This malware not only targets individuals but also infiltrates social media platforms and messaging apps, indicating a comprehensive effort to surveil online activities and communications.

The targets of these capabilities presents an interesting puzzle. Tehran's isolated focus on domestic surveillance is indicative of an

inconsistency in its overall national security architecture whereby it has failed, at least so far, to replicate its forward defense doctrine in its cybersecurity strategy. This is not to suggest that it has no offensive cyber capabilities, some of which are both well **documented (https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134)** and analyzed **(https://go.recordedfuture.com/hubfs/reports/cta-2024-0125.pdf)** . However, it seems that it has devoted much of its efforts and resources to developing surveillance capabilities suitable for domestic use and consequently depriving itself of the ability to detect and deter cyber threats from external actors in advance.

Stated broadly, Iran's national security strategy rests on two fundamental pillars. The first pillar is to leverage its geographical advantage to build an offensive capability centered around **mid- and long-range missiles (https://www.fdd.org/analysis/2023/02/15/arsenal-assessing-the-islamic-republic-of-irans-ballistic-missile-program/)** capable of striking targets both nearby and afar. The second one is hinged on cultivating a deterrence posture by **supporting (https://thesoufancenter.org/intelbrief-2023-november-3/)** ideologically aligned groups hostile to U.S. and Israeli interests in its vicinity. This latter aspect aligns with Tehran's objective of exerting influence rather than seeking outright control over neighboring states' affairs.

These proxy groups serve multiple purposes for Iran. They provide intelligence on adversaries' movements, hinder their interests when deemed necessary, and influence the political orientation of neighboring countries. By empowering these groups to become influential players in regional politics, Iran ensures that its neighbors either buttress its strategic interests or, at the very least, refrain from policies that are in direct contradiction to those interests. By outsourcing military engagements to non-Iranian actors, the Iranian regime also mitigates the risk of the type of **domestic backlash (https://www.jstor.org/stable/41409805)** commonly associated with military casualties.

In stark contrast to its approach on the regional stage, the regime's domestic agenda adheres to a **common authoritarian pattern (https://protectdemocracy.org/wp-content/uploads/2022/06/the-authoritarian-playbook-how-reporters-can-contextualize-and-cover-authoritarian-threats-as-distinct-from-politics-as-usual-1.pdf)** ; that is, maintaining full control over all aspects of public life. Recognizing their constrained resources—itself a direct consequence of its foreign policy priorities and the ensued Western-led sanction regimes—Iranian authorities predominantly perceive cyberspace and AI as tools for domestic manipulation and surveillance. This approach was **legislated (https://www.irna.ir/news/85269008/%25D9%2588%25D8%25B2%25D8%25A7%25D8%25B1%25D8%25AA-%25D8%25A7%25D8%25B1%25D8%25AA%25D8%25A8%25D8%25A7%25D8%25B7%25D8%25A7%25D8%25AA-%25D9%2585%25DA%25A9%25D9%2584%25D9%2581-%25D8%25A8%25D9%2587-%25D9%2587%25D9%2585%25DA%25A9%25D8%25A7%25D8%25B1%25DB%258C-%25D8%25A8%25D8%25A7-%25D9%2588%25D8%25B2%25D8%25A7%25D8%25B1%25D8%25AA-%25D8%25A7%25D8%25B7%25D9%2584%25D8%25A7%25D8%25B9%25D8%25A7%25D8%25AA-%25D8%25A8%25D8%25B1%25D8%25A7%25DB%258C-%25D8%25A7%25D9%2585%25D9%2586%25DB%258C%25D8%25AA-%25D8%25B3%25D8%25A7%25DB%258C%25D8%25A8%25D8%25B1%25DB%258C)** late last year by the Iranian Parliament into a law requiring the Ministry of Information and Communications Technology of Iran to unconditionally share all user data and information with the security forces.

In other words, while officials acknowledge the **significance (https://iranthinktanks.com/artificial-intelligence-and-its-future-implications-on-national-security-issues/)** of cyber tools and AI for foreign policy, they are acutely aware of the country's financial and scientific limitations that severely limit their full utilization in these arenas. Consequently, cyberspace and AI are **primarily seen (https://quarterly.risstudies.org/article_166567_a6d511e3f55bd401c23bead7f9e18059.pdf)** as instruments for reinforcing the government's **narratives ()** , shaping public perceptions and assisting the government to maintain absolute control over the society. For instance, a recently **broadcasted (https://www.khabaronline.ir/news/1851761/%25D8%25A8%25D8%25A8%25DB%258C%25D9%2586%25DB%258C%25D8%25AF-%25D8%25AD%25D8%25B1%25DA%25A9%25D8%25AA-%25D8%25B9%25D8%25AC%25DB%258C%25D8%25A8-%25D8%25B5%25D8%25AF%25D8%25A7%25D9%2588%25D8%25B3%25DB%258C%25D9%2585%25D8%25A7-%25D9%2585%25D8%25B5%25D8%25A7%25D8%25AD%25D8%25A8%25D9%2587-%25DA%25A9%25D8%25B1%25DB%258C%25D8%25B3%25D8%25AA%25DB%258C%25D8%25A7%25D9%2586%25D9%2588-%25D8%25B1%25D9%2588%25D9%2586%25D8%25A7%25D9%2584%25D8%25AF%25D9%2588-%25D8%25A8%25D9%2587-%25D8%25B2%25D8%25A8%25D8%25A7%25D9%2586)** deepfake interview featuring Portuguese football sensation Cristiano Ronaldo has the player—who signed a **$200 million a year contract (https://www.nbcsports.com/soccer/news/cristiano-ronaldo-signs-200-million-per-year-deal-with-al-nassr-report)** last year—discussing his financial challenges in an apparent attempt to normalize everyday Iranians' struggles of managing family expenses and the ongoing devaluation of Iranian riyal.

Furthermore, and arguably more significantly, investing in covert surveillance capabilities targeted at an Iranian audience offers a more

discreet and therefore effective method **(https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism)** of exerting influence over society and preserving a grip on power. Added to this is the so called export potential of its domestically produced surveillance softwares and systems as a lucrative source of income for the government. For instance, the recently revealed EyeSpy **(https://www.bitdefender.com/files/News/CaseStudies/study/427/Bitdefender-PR-Whitepaper-EyeSpyVPN-creat625-en-EN.pdf)** , an Iranian produced VPN laced with malware that enables the regime to monitor searches and conversations online, would be an attractive option for authoritarian regimes with limited budgetary resources. Cut off from global supply chains, Iran has been compelled to cultivate a domestic technological infrastructure to meet its security and commercial demands. With the added factors of a weakened currency, low labor and production costs, relaxed export policies, and a proactive stance in leveraging its expertise for financial gain and influence, Tehran now stands in a favorable position to promote its technology as a more economical substitute for Western counterparts.

Last but not least, there is the **dual benefit (https://community.ibm.com/community/user/security/blogs/albert-puah/2023/04/05/dual-intent-tools-commonly-used-by-hackers-and-how)** in developing surveillance technologies for domestic purposes in that they can subsequently be repurposed for deployment into Iran's adversaries systems and networks. Developing sophisticated offensive capabilities risks drawing international scrutiny and inviting further sanctions, potentially heightening the threat perceptions of Tehran's neighbors. This, in turn, may accelerate the **ongoing cyber arm race in the region (https://www.tandfonline.com/doi/full/10.1080/14751798.2024.2302699)** by prompting neighboring states to allocate substantial resources towards countering perceived Iranian capabilities. Given these competing priorities and resource constraints, the regime views investment in domestic surveillance as a more cost-effective and immediate means of maintaining control and influence while it continues to rely on its proxies for foreign intelligence/influence.

Overall, Iran's approach towards cybersecurity and artificial intelligence reflects complex dynamics at the intersection of national security strategy, domestic control, and resource limitations. While the nation's forward defense doctrine suggests that Tehran might prioritize robust offensive cyber capabilities, the reality of limited resources and widespread public discontent has led Iranian officials to primarily view cyber tools as both cost effective and discrete means for further strengthening of their already tight grip over the society. This focus on surveillance, with political dissidents as its primary target, highlights the regime's authoritarian tendencies and its reliance on technological innovation for the sole purpose of regime/internal security.

It must be noted, however, that the possibility of refitting some of the surveillance technology to serve both domestic control and potential foreign policy objectives underscores the high degree of pragmatism amongst Iranian strategists whose decade long struggle against Western sanctions has forced them to think and act innovatively. As such, to better comprehend the development and utilization of cyberspace and AI in Iran, one needs to reflect not only strategic imperatives but also the regime's broader authoritarian agenda and the constraints it faces on the international stage. ❖

RECOMMENDED

BRIEF ANALYSIS

The Continuing Threat of ISIS in Iraq after the Withdrawal of the International Coalition

Apr 4, 2024

◆

Omar Dhabian

(/policy-analysis/continuing-threat-isis-iraq-after-withdrawal-international-coalition)

BRIEF ANALYSIS

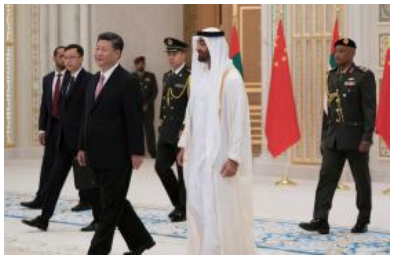
Curbing Outside Intervention in the Sudan War

Apr 4, 2024

◆

Jonathan Campbell-James

(/policy-analysis/curbing-outside-intervention-sudan-war)



BRIEF ANALYSIS

G42 and the China-UAE-U.S. Triangle

Apr 3, 2024

◆

Andrew G. Clemmensen,
Rebecca Redlich,
Grant Rumley

(/policy-analysis/g42-and-china-uae-us-triangle)

TOPICS

Iran's Domestic Affairs (/policy-analysis/irans-domestic-affairs)

Iran's Foreign Policy (/policy-analysis/irans-foreign-policy)

REGIONS & COUNTRIES

Iran (/policy-analysis/iran)