THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Mariam Habib Matta
Department of Government
m.a.habib-matta@lse.ac.uk

PERIOD PADS ON CCTV CAMERAS: A CASE STUDY OF AI WEAPONISATION AGAINST FEMINIST RESISTANCE IN IRAN

Introduction

This research addresses the neglected intersection of AI mass surveillance and the impact on women's resistance in the Middle East. I spefically focus on the employment of AI to suppress feminist resistance against the compulsory hijab. Since 1979, veiling has been mandatory, and in 2005 the creation of the 'Morality Police'. Decades of protests, notably, 2009, 2017-8, and 2019-20 have ensued. Critically, recent protests after the murder of Mahsa Amini in 2022, has led to over 470 killed protestors and 18,000 jailed.

In 2023, a new AI weapon has been employed, the first officially announced; facial recognition of women improperly veiled.

The study delves into suppression strategies like facial recognition, automated Twitter bots, and the development of mass surveillance and social media profiling. I explore counterstrategies women employ, like VPNs; apps such as Nahoft and Gershad; and covering facial recognition cameras with period pads.

By doing so, the research aims to deepen our understanding of how the Iranian authorities' development of AI mass surveillance to target women's resistance movements creates a shift in the methods employed by women in their pursuit of change, as well as the novel obstacles faced by the feminist movement in the Middle East.

Weaponisation of AI In Iran for Suppression

Facial Recognition CCTV Cameras

Photo of FR Report [2]

In 2023, Iranian authorities have began using facial recognition technology in public places to suppress women who defy the compulsory hijab requirement.[1]

AI-powered systems compare unveiled women to Iran's digital surveillance apparatus, which has compiled biometric data used in National ID cards.

Facial recognition identifies them breaking modesty laws and sends a warning text message, and if the woman continues is placed under arrest.

Reports indicate the widespread installation of 15 million cameras across 28 cities in Iran.[3] Facial recognition is also utilised by traffic authorities to target women not wearing hijabs properly, even in their own vehicles.[4]

Social Media Profiling

Considering the knowledge gap, we can extrapolate from already developed tech and strategy. It is already known that Iran has monitored 8 million Facebook accounts with 'new software' to screen for activity that contravenes the Islamic Republic's moral code.[5]

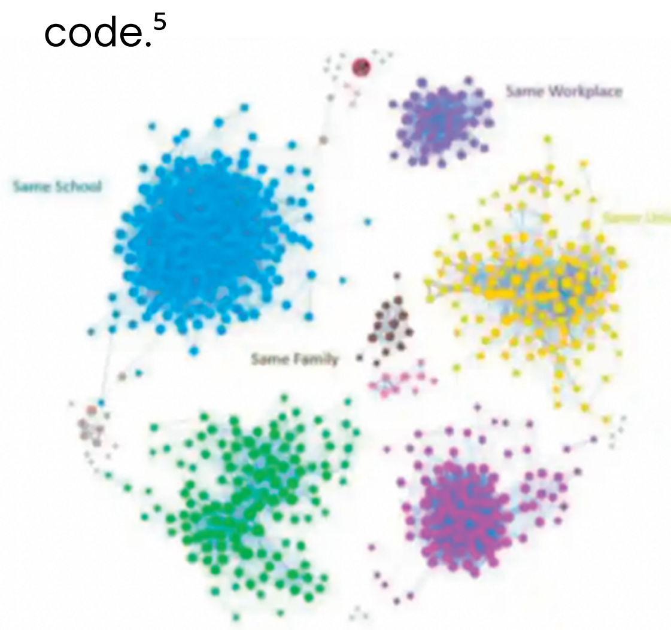


Diagram Which shows the ML connections Voyager makes when profiling.[6]

For example, Voyager, which visualises individual social media connections and analyses profile content. Used to mass create surveillance profiles of their ideological affiliations and predicted beliefs. Voyager has already begun application in MENA.[7]

Mass Internet Surveillance

A significant shift in Iranian surveillance practices is adoption of machine learning programmes. Transition has coincided with Sino-Iranian agreements with Chinese company, Tiandy, infamous for its 'tiger chair torture' and surveillance of Uighur Muslims.[8]

Due to the sensitive nature exact AI integration is unknown but, we can infer from currently known tools[9]:

URL Blacklisting- blocks access to websites that the Iranian authorities deem undesirable, with machine learning algorithms, it is faster to censor information.

Content Control Software- Allows authorities to restrict access to online content which would be much faster using ML algorithms.

Traffic Analysis- monitors metadata and patterns of political dissent activities. AI would make it easier to comb through more data.

AI Driven Twitter Bots

AI-driven Twitter bots work to suppress freedom of speech and dissent, which is especially damaging since hashtag activism is critical for the movement.

Figure 1. Even since 2019-2020 Protests in Iran, the red and orange lines show very high botness levels, where those tweets and activity on Twitter are very likely to be bots.[10]

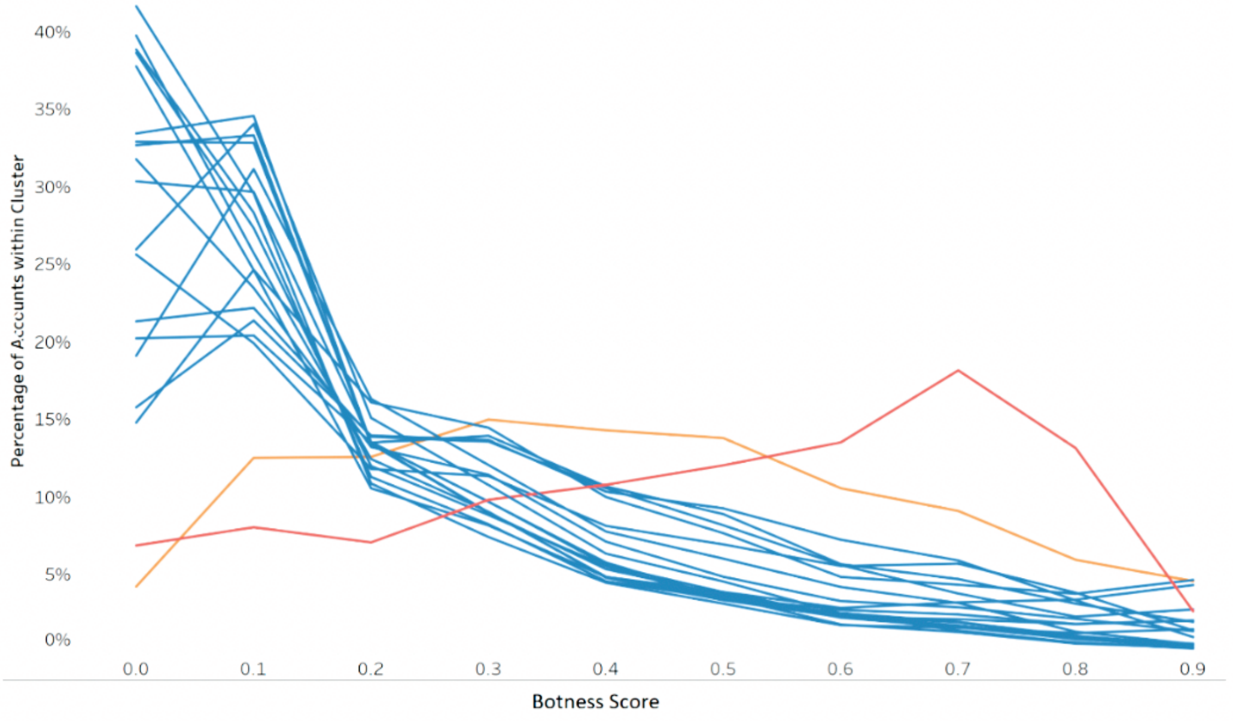
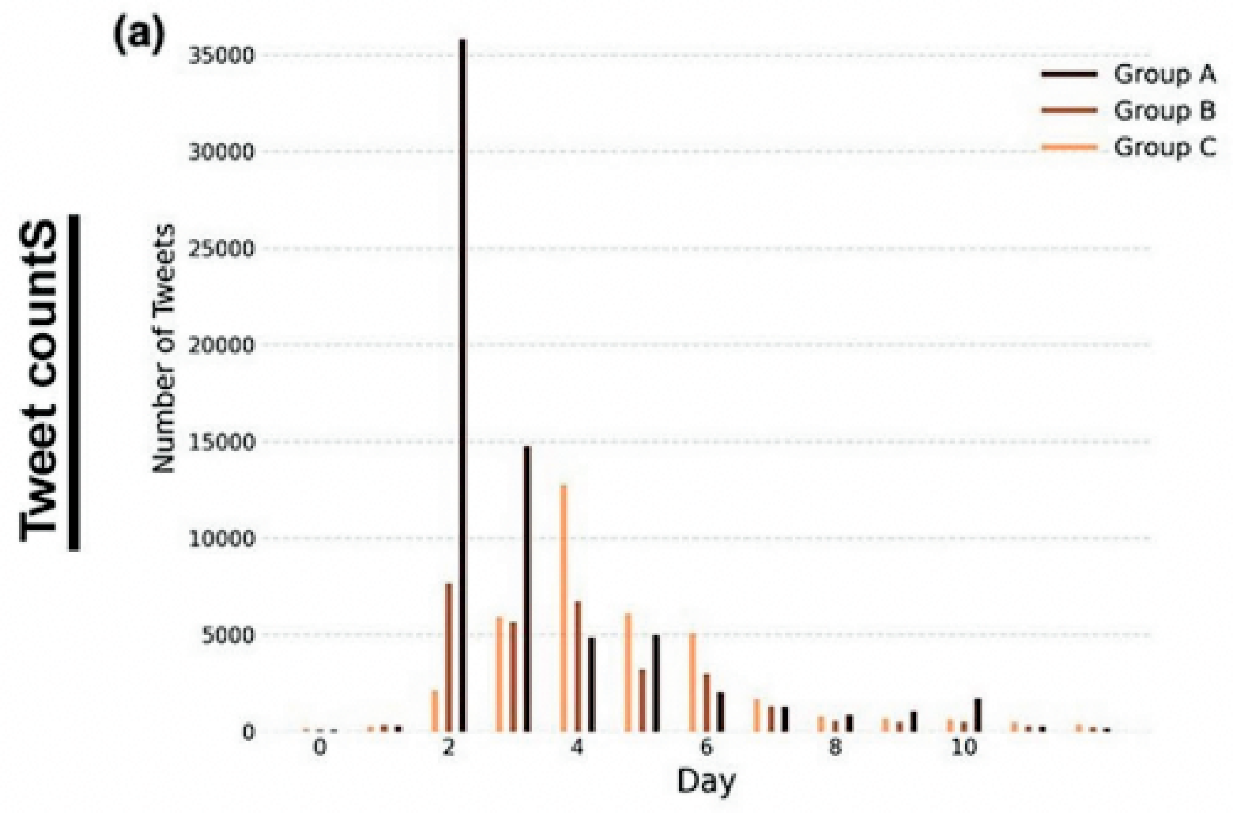


Figure 2. Pro-Regime/Pro-Compulsory Hijab Twitter Activity has much higher CAP Twitter activity. A Botometer, which is a machine-learning algorithm that measures CAP (Complete Automation Probability) which is inauthentic Twitter activity.[11]



Counterstrategies by Women

PERIOD PADS

Covering Facial Recognition CCTV with period pads
Image from a Metro in Tehran, where women directly block the surveillance of CCTV [12]

NAHOFT

Means 'hidden' in Farsi, and encrypts text to jumble of random words. Favoured by journalists, activists, and feminist resistors to avoid digital surveillance.[13]

GERSHAD

Collective mapping tool, where women can pin morality police patrols to encourage women to avoid or be alert nearby. It has also been used to report location of riot police.[14]

VPNS

Many Iranians use VPNs despite them being forbidden and blocked by the Iranian authorities. VPNs hide information from ISPs, which offers a slightly higher chance of avoiding surveillance and targeting.[15]

Concluding Findings

- My research has aimed to signify the emerging significance of AI as a weaponised barrier for feminist resistance in the Middle East, and I find there are two significant implications.

1. AI highlights the gap in approaching feminist resistance. For instance, in Iran, women's oppression through compulsory hijab cannot be solved in simple solutions like solely removing the Morality Police. AI facial recognition, and mass internet surveillance has shown that human monitoring can be more efficiently replaced by an algorithm.
2. Younger generations are in a higher risk of danger due to their reliance on digitised modes of resistance. Social media profiling, surveillance, and infiltration on social media platforms like Twitter, show that they operate in more precarious positions. I suggest, developing clearer methods of communication that are further diversified than digital alone.

References

[1] Forbes (2023). 'Iran Installs Cameras For Morality Police To Identify Women Defying Hijab Law'. https://www.forbes.com/sites/mattnovak/2023/04/08/iran-installs-cameras-for-morality-police-to-identify-women-defying-hijab-law/.
[2] Fact Nameh. (2023). هوش مصنوعی کشف حجاب. https://factnameh.com/fa/fact-checks/2023-04-18-iran-facial-recognition-surveillance-hijab.
[3] The Diplomat. (2023). How China Boosts Iran's Digital Crackdown. https://thediplomat.com/2022/10/how-china-boosts-irans-digital-crackdown/.
[4] Završnik, A. et al. (2021). Automating Crime Prevention, Surveillance and Military Operations. Springer Cham.
[5] Reuters. (2015). 'Iran's Guards Increase Monitoring of Social Media - State TV'. https://www.reuters.com/article/uk-iran-internet-idUKKBN0LY1XT20150302
[6] The Guardian, et al. (2021). 'Revealed: The Software That Studies Your Facebook Friends to Predict Who May Commit a Crime'. https://www.theguardian.com/us-news/2021/nov/17/police-surveillance-technology-voyager.
[7] Ibid.
[8]MIT Technology Review. (2023). 'This Huge Chinese Company Is Selling Video Surveillance Systems to Iran'. https://www.technologyreview.com/2021/12/15/1042142/chinese-company-tiandy-video-surveillance-iran/.
[9] Akbari, A. et al. (2019) Platform Surveillance and Resistance in Iran and Russia: The Case of Telegram. Surveillance & society. 17(1).
[10] Dehghan, E. et al. (2020). Investigating Bots and Coordinated Influence Campiagns in Twitter Discussions of the 2019-20 Iran Protests. AoIR Selected Papers of Internet Research.
[11] Farzam, A. et al. (2023). Opinion manipulation on Farsi Twitter. Sci Rep 13(333).
[12] Middle East Eye. (2023). Iranians Use New Tool to Fight Surveillance of Women: Sanitary Pads. http://www.middleeasteye.net/news/iran-women-surveillance-tool-fight-sanitary-pads.
[13] Context. (2023). Protesters - and Police - Deploy Tech in Fight for Future of Iran. https://www.context.news/surveillance/protesters-and-police-deploy-tech-in-fight-for-future-of-iran.
[14] Ibid.
[15] Wulf, V. et al. (2022) The Personal is the Political: Internet Filtering and Counter Appropriation in the Islamic Republic of Iran. Computer Supported Cooperative Work 31(2).