Australian Supporters of Democracy in Iran

Submission

To the Select Committee on Foreign Interference through Social Media inquiry into the risk posed to Australia's democracy by foreign interference through social media.

February 2023

PO Box 73, Mortdale NSW 2223

Introduction

Australian Supporters of Democracy in Iran was formed in 2004. It is not a "Parliamentary Friends of Democratic Iran", and while membership of federal and state MPs is a high priority, it has always had membership from trade unions, churches, anti-war and human rights activists.

The Objectives are:

- Support democracy in Iran, and the principles of the National Council of Resistance of Iran (NCRI), and in particular its 10-Point Plan attached.
- Support of peace, stability and freedom
- Support the rights of women against fundamentalism and discrimination.

We welcome this opportunity to make a submission to the Senate Select Committee on Foreign Interference through Social Media in relation to the dramatic situation unfolding now in Iran, responding to the Terms of Reference, and making our own recommendations for the Committee and the Government to consider.

The use of social media for purposes that undermine Australia's democracy and values, including the spread of misinformation and disinformation

Australia's democracy is based on freedom of the media, freedom of expression, freedom of assembly, freedom of association and elections and referenda conducted by secret ballot by independent electoral commissions with each adult citizen able to cast one vote of equal value to that of all other voters.

Social media is a relatively new dimension of the media and it is now well-known that false information can be created and targeted at specific demographic groups in the community through social media to influence voting outcomes, with the most notorious case being the various campaigns conducted by Cambridge Analytica.

The Iranian government has invested heavily in cyber surveillance and created its own messaging apps to enable it to monitor dissident opinions and to communicate its own "information".

A November 2022, report by Deutche Welle gives a broad overview:

> Internet penetration in Iran is over 84%, according to World Bank estimates. According to data website Globalstats' numbers for October 2022, nearly 27% of Iranians use Pinterest, followed by Instagram (17%), Reddit (13.3%) and Twitter (10.4%). Telegram is also very popular among Iran's youth, with more than 40 million users in the country, Telegram founder Pavel Durov has said. That is almost half of the country's population - 90 million people live in Iran.
>
> Instagram and Whatsapp were popular until September, when the government curbed access to the platforms. In 2021, 89 % of Iranians had been using Instagram.
>
> The regime in Teheran has complete control over all communications in the country, be it news, internet, or social media, says Mahdi Saremifar, a science and technology journalist based in Regina, Canada.
>
> "Mobile network operators and internet service providers are run by private companies, which are monitored by Ayatollah Khamenei through a complex network of commercial and

> investment companies and ultimately four economic institutions: the Mostazafan Foundation, Astan Quds Razavi, Khatam al-Anbiya Construction Headquarter IRGC (GHORB) and Execution of Imam Khomeini's Order (EIKO)," he explains.
>
> People in Iran are therefore dependent on social networks for unbiased news and access the internet through virtual private networks (VPNs) to sidestep the regime's control. And rather than stifling communication, increased surveillance has only fueled protesters' anger. Teheran's heavy-handed treatment of the protesters, which include arresting, torturing and sentencing offenders to death, has actually given a direction to public opinion, Saremifar says.
>
> As a result, social media has assumed two crucial functions in the country, the journalist adds. The first is, to inform people about what is really going on, and record events for human rights institutions, for example. The second purpose is to serve as a tool for coordinating people, for organizing protests on a daily basis.[1]

Australia's Cyber Security Centre stated in November 2021:

> The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have observed an Iranian government-sponsored advanced persistent threat (APT) group exploit Fortinet vulnerabilities since at least March 2021, and a Microsoft Exchange ProxyShell vulnerability since at least October 2021 to gain access to systems in advance of follow-on operations, which include deploying ransomware. ACSC is also aware this APT group has used the same Microsoft Exchange vulnerability in Australia.
>
> The Iranian government-sponsored APT actors are actively targeting a broad range of victims across multiple U.S. critical infrastructure sectors, including the Transportation Sector and the Healthcare and Public Health Sector, as well as Australian organizations. FBI, CISA, and ACSC assess the actors are focused on exploiting known vulnerabilities rather than targeting specific sectors. These Iranian government-sponsored APT actors can leverage this access for follow-on operations, such as data exfiltration or encryption, ransomware, and extortion.[2]

Australian security agencies have disrupted a foreign interference plot by Iran that was targeting an Iranian-Australian on Australian soil, the Department of Home Affairs have said in their submission to this Inquiry.

The plot allegedly included individuals monitoring the home of a critic of the Iranian regime and extensively researching the person and their family.[3]

When Iranian-Australians in particular have been gathering to support the popular uprising inside Iran, they have been subjected to cyber surveillance and in many cases, their relatives in Iran have been interrogated and threatened, and demands placed on their Australian relatives to cease their protest efforts here in Australia. This is a direct attack on the freedom of assembly and freedom of expression in Australia, facilitated by social media.

[1] https://www.dw.com/en/social-media-iran-unrest/a-63913630.
[2] https://www.cyber.gov.au/acsc/view-all-content/alerts/iranian-government-sponsored-apt-cyber-actors.
[3] https://www.theguardian.com/australia-news/2023/feb/14/australia-foils-iran-surveillance-plot-and-vows-to-bring-foreign-interference-into-the-light.

Responses to mitigate the risk posed to Australia's democracy and values, including by the Australian Government and social media platforms

On January 25, 2023, a spokeswoman for Foreign Minister Penny Wong told the ABC, "The Australian government is deeply concerned by reports of foreign interference, including the harassment and intimidation of Australians online and in-person".

"We have raised our concerns about foreign interference directly to the Iranian regime in no uncertain terms," she said.

"Australia will continue to work domestically to keep Australians safe from foreign interference and with our like-minded partners to apply pressure on the Iranian regime over its egregious human rights abuses."[4]

While the Minister took decisive action to sanction individuals and entities in Iran on December 10, 2022, and February 1,2023, these actions were not related to the use of social media to interfere with Australian democracy.

International policy responses to cyber-enabled foreign interference and misinformation

A recent McKinsey & Company report tried to benchmark international efforts to manage cybersecurity threats.[5]

It argued that there are five basic elements to an effective cybersecurity strategy:

- a dedicated national cybersecurity agency (NCA)
- a National Critical Infrastructure Protection program
- a national incident response and recovery plan
- defined laws pertaining to all cybercrimes
- a vibrant cybersecurity ecosystem

However, none of these relate strongly to political interference through social media.

So this is an area of policy and governance which is under-developed, including in Australia.

Only civil law appears to have an impact at the margins on abuse of social media, mainly through libel and defamation cases. Creation of social media accounts is regulated by the private sector platforms involved, leading to a culture of pseudonyms and fake accounts.

The extent of compliance with existing Australian laws and regulations

According to the Australian Human Rights Commission, social media postings can be against the law if they discriminate against, harass, bully or racially vilify a person.[6]

[4] https://www.abc.net.au/news/2023-01-25/australia-iran-irgc-cyber-attacks-senate-inquiry-human-rights/101886648.
[5] https://www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks.
[6] https://humanrights.gov.au/quick-guide/12098.

Discrimination occurs when a person is treated less favourably than another person because of a particular attribute they have. Harassment or bullying can amount to discrimination in some circumstances.

Inappropriate posts, comments or content shared on social media can amount to sexual harassment.

Clearly, threats and incitement to violence in social media posts would also be unlawful, and would be criminal rather than civil matters.

However, the extent of abuse of individuals on social media in Australia is enormous, with little effective protection available to victims other than to somehow switch off or develop an alternative online identity.

Therefore, organised social media surveillance and abuse in Australia by Iranian government agencies is largely uncontrolled.

Recommendations

1. The Australian Cyber Security Centre should create a unit capable of:
   - directly monitoring internet and social media traffic from Iran to Australia
   - identifying Iranian government agencies operating social media in Australia
   - receiving complaints from Australian citizens and residents of cyber abuse relating to Iran
   - reporting cases of illegal social media activity to police or prosecuting agencies.
2. Since the Iranian Revolutionary Guards Corp (IRGC) is identified as a major owner of social media in Iran, it should be held accountable for the abuse cases in which it is identified. Since it cannot be tried in an Australian court, the Australian government should take other action against it where possible. If Australian law does not allow a “state entity” to be listed as a terrorist organisation, the law should be amended to enable this. The IRGC is not the Iranian military, which has its own assets and command structures. The IRGC is directly controlled by the Supreme Leader, Ayatollah Khamenei, much as the German SS was loyal directly to Adolf Hitler, not to the German Army high Command.

###